TABLE OF CONTENTS

ABOUT THIS GUIDE

Chapter 1, INTRODUCTION
  1.3.1 Basic Conventions ........................................................................................................ .............................1-10
  1.4.1 Moving the Cursor on the Command Line .................................................................................... .............1-10
  1.4.2 Completing a Partial Command Name ........... ...........................................................................................1-11
  1.4.3 Command Output Pagination ................................................................................................ ....................1-12
  1.5.1 Creating Profiles ........................................................................................................ ................................1-12
  1.5.2 Changing the default profile by creating vlan 150 and mapping to ge3 Physical interface ...............1-13
  1.5.3 Enabling Remote Administration ...................................................................................................... 1-13

Chapter 2, USER EXEC MODE COMMANDS
  2.1.1 captive-portal-page-upload ............................................................................................... ...........................2-5
  2.1.2 change-passwd ............................................................................................................ ...............................2-8
  2.1.3 clear .................................................................................................................... .........................................2-9
  2.1.4 clock .................................................................................................................... ......................................2-20
  2.1.5 cluster .................................................................................................................. ......................................2-21
  2.1.6 connect .................................................................................................................. ....................................2-22
  2.1.7 create-cluster ........................................................................................................... ..................................2-23
  2.1.8 crypto ................................................................................................................... ......................................2-25
  2.1.9 crypto-cmp-cert-update ................................................................................................... ..........................2-34
  2.1.10 database ................................................................................................................ ..................................2-35
  2.1.11 database-backup ........................................................................................................ .............................2-36
  2.1.12 database-restore ........................................................................................................ .............................2-37
  2.1.13 device-upgrade ........................................................................................................ ..............................2-38
  2.1.14 disable ................................................................................................................. ....................................2-48
  2.1.15 enable .................................................................................................................. ....................................2-49
  2.1.16 file-sync ............................................................................................................... ....................................2-50
  2.1.17 join-cluster ............................................................................................................ ...................................2-52
  2.1.18 l2tpv3 .................................................................................................................. .....................................2-54
  2.1.19 logging ................................................................................................................. ....................................2-56
  2.1.20 mint .................................................................................................................... ......................................2-58
  2.1.21 no ...................................................................................................................... .......................................2-60
  2.1.22 on ...................................................................................................................... .......................................2-62
### Chapter 3, PRIVILEGED EXEC MODE COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>3-6</td>
</tr>
<tr>
<td>boot</td>
<td>3-8</td>
</tr>
<tr>
<td>captive-portal-page-upload</td>
<td>3-9</td>
</tr>
<tr>
<td>cd</td>
<td>3-12</td>
</tr>
<tr>
<td>change-passwd</td>
<td>3-13</td>
</tr>
<tr>
<td>clear</td>
<td>3-14</td>
</tr>
<tr>
<td>clock</td>
<td>3-27</td>
</tr>
<tr>
<td>cluster</td>
<td>3-28</td>
</tr>
<tr>
<td>configure</td>
<td>3-29</td>
</tr>
<tr>
<td>connect</td>
<td>3-30</td>
</tr>
<tr>
<td>copy</td>
<td>3-31</td>
</tr>
<tr>
<td>cpe</td>
<td>3-32</td>
</tr>
<tr>
<td>create-cluster</td>
<td>3-34</td>
</tr>
<tr>
<td>crypto</td>
<td>3-36</td>
</tr>
<tr>
<td>crypto-cmp-cert-update</td>
<td>3-45</td>
</tr>
<tr>
<td>database</td>
<td>3-46</td>
</tr>
<tr>
<td>database-backup</td>
<td>3-47</td>
</tr>
<tr>
<td>database-restore</td>
<td>3-48</td>
</tr>
<tr>
<td>delete</td>
<td>3-49</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>3-50</td>
</tr>
<tr>
<td>diff</td>
<td>3-57</td>
</tr>
<tr>
<td>dir</td>
<td>3-58</td>
</tr>
<tr>
<td>disable</td>
<td>3-59</td>
</tr>
<tr>
<td>edit</td>
<td>3-60</td>
</tr>
<tr>
<td>enable</td>
<td>3-61</td>
</tr>
<tr>
<td>erase</td>
<td>3-62</td>
</tr>
<tr>
<td>ex3500</td>
<td>3-64</td>
</tr>
<tr>
<td>factory-reset</td>
<td>3-71</td>
</tr>
<tr>
<td>file-sync</td>
<td>3-75</td>
</tr>
<tr>
<td>format</td>
<td>3-50</td>
</tr>
<tr>
<td>halt</td>
<td>3-78</td>
</tr>
<tr>
<td>join-cluster</td>
<td>3-79</td>
</tr>
<tr>
<td>i2tpv3</td>
<td>3-81</td>
</tr>
<tr>
<td>logging</td>
<td>3-83</td>
</tr>
<tr>
<td>mint</td>
<td>3-85</td>
</tr>
<tr>
<td>mkdir</td>
<td>3-87</td>
</tr>
<tr>
<td>more</td>
<td>3-88</td>
</tr>
<tr>
<td>no</td>
<td>3-89</td>
</tr>
</tbody>
</table>
Chapter 4, GLOBAL CONFIGURATION COMMANDS

4.1.1 aaa-policy .............................................................. 4-9
4.1.2 alias ......................................................................... 4-10
4.1.3 aaa-tacacs-policy ................................................... 4-17
4.1.4 ap621 .................................................................. 4-18
4.1.5 ap622 .................................................................. 4-19
4.1.6 ap650 .................................................................. 4-20
4.1.7 ap6511 ................................................................. 4-21
4.1.8 ap6521 ................................................................. 4-22
4.1.9 ap6522 ................................................................ 4-23
4.1.10 ap6532 ............................................................... 4-24
4.1.11 ap6562 ............................................................... 4-25
4.1.12 ap71xx ............................................................... 4-26
4.1.13 ap7502 ............................................................... 4-27
4.1.14 ap7522 ............................................................... 4-28
4.1.15 ap7532 ............................................................... 4-29
4.1.16 ap7562 ............................................................... 4-30
4.1.17 ap81xx ............................................................... 4-31
4.1.18 ap82xx ............................................................... 4-32
4.1.19 application ........................................................ 4-33
4.1.20 application-policy .............................................. 4-42
4.1.21 association-acl-policy ........................................... 4-59
4.1.22 auto-provisioning-policy ..................................... 4-60
4.1.23 bgp .................................................................. 4-61
4.1.24 bonjour-gw-discovery-policy ............................ 4-63
4.1.25 bonjour-gw-forwarding-policy ....................... 4-65
4.1.26 bonjour-gw-query-forwarding-policy .............. 4-66
4.1.27 captive portal .................................................... 4-67

3.1.39 on ........................................................................ 3-91
3.1.40 opendns ............................................................ 3-92
3.1.41 page ..................................................................... 3-94
3.1.42 ping ...................................................................... 3-95
3.1.43 ping6 ................................................................. 3-97
3.1.44 pwd ...................................................................... 3-98
3.1.45 re-elect .............................................................. 3-99
3.1.46 reload ................................................................. 3-100
3.1.47 rename ............................................................... 3-105
3.1.48 mkdir ................................................................. 3-106
3.1.49 self ..................................................................... 3-107
3.1.50 ssh ...................................................................... 3-108
3.1.51 t5 ......................................................................... 3-109
3.1.52 telnet ................................................................. 3-111
3.1.53 terminal ............................................................ 3-112
3.1.54 time-it .............................................................. 3-113
3.1.55 traceroute ........................................................ 3-114
3.1.56 traceroute6 ........................................................ 3-115
3.1.57 upgrade ............................................................ 3-116
3.1.58 upgrade-abort .................................................. 3-120
3.1.59 watch ................................................................. 3-121
3.1.60 exit ..................................................................... 3-122
3.1.61 smart-cache ........................................................ 3-123
3.1.62 virtual-machine .............................................. 3-124
3.1.63 raid ................................................................. 3-133
4.1.28 clear .................................................................4-107
4.1.29 client-identity ..............................................4-108
4.1.30 client-identity-group .....................................4-116
4.1.31 clone .................................................................4-123
4.1.32 crypto-cmp-policy ........................................4-124
4.1.33 customize .........................................................4-125
4.1.34 device .................................................................4-136
4.1.35 device-categorization ...................................4-138
4.1.36 dhcp-server-policy ........................................4-143
4.1.37 dhcpv6-server-policy ....................................4-144
4.1.38 dns-whitelist ................................................4-146
4.1.39 end .................................................................4-151
4.1.40 event-system-policy .......................................4-152
4.1.41 ex3500 ..............................................................4-167
4.1.42 ex3500-management-policy .........................4-174
4.1.43 ex3500-qos-class-map-policy .........................4-192
4.1.44 ex3500-qos-policy-map ..................................4-200
4.1.45 ex3524 ..............................................................4-214
4.1.46 ex3548 ..............................................................4-216
4.1.47 firewall-policy ................................................4-217
4.1.48 global-association-list ....................................4-219
4.1.49 guest-management .........................................4-221
4.1.50 host .................................................................4-232
4.1.51 inline-password-encryption .............................4-233
4.1.52 ip .....................................................................4-234
4.1.53 ipv6 .................................................................4-236
4.1.54 ipv6-router-advertisement-policy ..................4-237
4.1.55 l2tpv3 ...............................................................4-255
4.1.56 mac .................................................................4-257
4.1.57 management-policy .......................................4-258
4.1.58 meshpoint .........................................................4-260
4.1.59 meshpoint-qos-policy ....................................4-262
4.1.60 mint-policy ........................................................4-263
4.1.61 nac-list .............................................................4-264
4.1.62 no .................................................................4-270
4.1.63 nsight-policy ..................................................4-274
4.1.64 passpoint-policy .............................................4-283
4.1.65 password-encryption ....................................4-285
4.1.66 profile .............................................................4-286
4.1.67 radio-qos-policy .............................................4-290
4.1.68 radius-group ................................................4-291
4.1.69 radius-server-policy .......................................4-292
4.1.70 radius-user-pool-policy .................................4-293
4.1.71 rename ..........................................................4-294
4.1.72 rf-domain .........................................................4-297
4.1.73 rfs4000 ............................................................4-329
4.1.74 rfs6000 ............................................................4-330
4.1.75 rfs7000 ............................................................4-331
4.1.76 nx45xx .............................................................4-332
4.1.77 nx5500 .............................................................4-333
4.1.78 nx65xx .............................................................4-334
4.1.79 nx75xx .............................................................4-335
4.1.80 nx9000 .............................................................4-336
4.1.81 roaming-assist-policy ....................................4-337
4.1.82 role-policy .................................................4-338
Chapter 5, COMMON COMMANDS

5.1.1 clrscri ................................................................. 5-3
5.1.2 commit ................................................................. 5-4
5.1.3 exit ................................................................. 5-5
5.1.4 help ................................................................. 5-6
5.1.5 no ................................................................. 5-9
5.1.6 revert ............................................................... 5-12
5.1.7 service .............................................................. 5-13
5.1.8 show ............................................................... 5-50
5.1.9 write ............................................................... 5-52

Chapter 6, SHOW COMMANDS

6.1.1 show ............................................................... 6-6
6.1.2 adoption ......................................................... 6-12
6.1.3 boot ............................................................... 6-16
6.1.4 bonjour .......................................................... 6-17
6.1.5 captive-portal .................................................. 6-18
6.1.6 captive-portal-page-upload ......................... 6-20
6.1.7 cdp .................................................................. 6-21
6.1.8 classify-url ..................................................... 6-23
6.1.9 clock .............................................................. 6-24
6.1.10 cluster ........................................................... 6-25
6.1.11 cmp-factory-certs ........................................ 6-26
6.1.12 commands .................................................... 6-27
6.1.13 context .......................................................... 6-28
6.1.14 critical-resources ........................................... 6-29
6.1.15 crypto ............................................................ 6-30
6.1.16 database ....................................................... 6-33
6.1.17 device-upgrade ............................................. 6-34
6.1.18 dot1x ........................................................... 6-37
6.1.19 dpi ............................................................... 6-39
6.1.20 environmental-sensor ................................. 6-42
6.1.21 event-history ................................................ 6-45
6.1.22 event-system-policy ..................................... 6-46
6.1.23 ex3500 .......................................................... 6-47
6.1.24 extdev ........................................................... 6-50
6.1.25 file .............................................................. 6-51
6.1.26 file-sync ........................................................ 6-52
6.1.27 firewall .........................................................................................................................6-54
6.1.28 global ..........................................................................................................................6-58
6.1.29 gre ...............................................................................................................................6-60
6.1.30 guest-registration ........................................................................................................6-61
6.1.31 interface .......................................................................................................................6-68
6.1.32 ip ..................................................................................................................................6-72
6.1.33 ip-access-list ...............................................................................................................6-80
6.1.34 ipv6 ............................................................................................................................6-82
6.1.35 ipv6-access-list ..........................................................................................................6-86
6.1.36 l2tpv3 ........................................................................................................................6-87
6.1.37 ldap-agent ................................................................................................................6-90
6.1.38 licenses .......................................................................................................................6-91
6.1.39 lldp ................................................................................................................................6-94
6.1.40 logging .......................................................................................................................6-95
6.1.41 mac-access-list .........................................................................................................6-96
6.1.42 mac-address-table ....................................................................................................6-97
6.1.43 mac-auth ...................................................................................................................6-98
6.1.44 mac-auth-clients .......................................................................................................6-100
6.1.45 mint ............................................................................................................................6-102
6.1.46 ntp ................................................................................................................................6-105
6.1.47 password-encryption ...............................................................................................6-107
6.1.48 pppoe-client .............................................................................................................6-108
6.1.49 privilege ....................................................................................................................6-109
6.1.50 radius ........................................................................................................................6-110
6.1.51 reload ........................................................................................................................6-112
6.1.52 rf-domain-manager .................................................................................................6-113
6.1.53 role ................................................................................................................................6-114
6.1.54 route-maps ...............................................................................................................6-115
6.1.55 rls ..................................................................................................................................6-116
6.1.56 running-config .........................................................................................................6-117
6.1.57 session-changes ......................................................................................................6-123
6.1.58 session-config ..........................................................................................................6-124
6.1.59 sessions .....................................................................................................................6-125
6.1.60 site-config-diff .......................................................................................................6-126
6.1.61 smart-rf ......................................................................................................................6-127
6.1.62 spanning-tree .........................................................................................................6-131
6.1.63 startup-config .........................................................................................................6-134
6.1.64 t5 ..................................................................................................................................6-135
6.1.65 terminal .....................................................................................................................6-141
6.1.66 timezone ..................................................................................................................6-142
6.1.67 traffic-shape ............................................................................................................6-143
6.1.68 upgrade-status .......................................................................................................6-145
6.1.69 version ......................................................................................................................6-147
6.1.70 vrrp ............................................................................................................................6-148
6.1.71 web-filter .................................................................................................................6-150
6.1.72 what ........................................................................................................................6-152
6.1.73 wireless .....................................................................................................................6-153
6.1.74 wwan ........................................................................................................................6-174
6.1.75 slot .............................................................................................................................6-175
6.1.76 smart-cache .............................................................................................................6-176
6.1.77 virtual-machine .......................................................................................................6-178
6.1.78 mirroring ..................................................................................................................6-181
6.1.79 raid ............................................................................................................................6-182
Chapter 7, PROFILES

7.1.1 adopter-auto-provisioning-policy-lookup ................................................................. 7-11
7.1.2 adoption .................................................................................................................. 7-12
7.1.3 alias ....................................................................................................................... 7-13
7.1.4 application-policy .................................................................................................. 7-20
7.1.5 area ...................................................................................................................... 7-21
7.1.6 arp ....................................................................................................................... 7-22
7.1.7 auto-learn-staging-config ..................................................................................... 7-24
7.1.8 autogen-uniqeid ................................................................................................. 7-25
7.1.9 autoinstall ............................................................................................................ 7-27
7.1.10 bluetooth-detection ......................................................................................... 7-28
7.1.11 bridge .............................................................................................................. 7-29
7.1.12 captive-portal .................................................................................................... 7-55
7.1.13 cdp ................................................................................................................... 7-56
7.1.14 cluster .............................................................................................................. 7-57
7.1.15 configuration-persistence ............................................................................... 7-60
7.1.16 controller ......................................................................................................... 7-61
7.1.17 critical-resource .............................................................................................. 7-65
7.1.18 crypto ............................................................................................................... 7-72
7.1.19 database-backup .............................................................................................. 7-133
7.1.20 device-upgrade ............................................................................................... 7-134
7.1.21 dot1x ............................................................................................................... 7-136
7.1.22 dpi ................................................................................................................... 7-138
7.1.23 dscp-mapping .................................................................................................. 7-140
7.1.24 email-notification ......................................................................................... 7-141
7.1.25 enforce-version ............................................................................................... 7-143
7.1.26 environmental-sensor ................................................................................... 7-144
7.1.27 events ............................................................................................................. 7-146
7.1.28 export .......................................................................................................... 7-147
7.1.29 file-sync ........................................................................................................ 7-148
7.1.30 floor .............................................................................................................. 7-149
7.1.31 gre .................................................................................................................. 7-150
7.1.32 http-analyze ................................................................................................... 7-162
7.1.33 http-analyze (NX45XX, NX65XX, and NX9000) ........................................... 7-164
7.1.34 interface ........................................................................................................ 7-167
7.1.35 ip .................................................................................................................... 7-347
7.1.36 ipv6 .............................................................................................................. 7-357
7.1.37 l2tpv3 ........................................................................................................ 7-361
7.1.38 l3e-lite-table ................................................................................................. 7-363
7.1.39 led .................................................................................................................. 7-364
7.1.40 led-timeout ................................................................................................. 7-365
7.1.41 legacy-auto-downgrade ........................................................................... 7-367
7.1.42 legacy-auto-update ...................................................................................... 7-368
7.1.43 lldp ............................................................................................................... 7-369
7.1.44 load-balancing ............................................................................................ 7-371
7.1.45 logging ........................................................................................................ 7-376
7.1.46 mac-address-table ...................................................................................... 7-378
7.1.47 mac-auth ..................................................................................................... 7-380
7.1.48 memory-profile ........................................................................................... 7-383
7.1.49 meshpoint-device ....................................................................................... 7-384
7.1.50 meshpoint-monitor-interval ...................................................................... 7-385
7.1.51 min-misconfiguration-recovery-time ......................................................... 7-386
7.1.52 mint .......................................................................................................... 7-387
7.1.53 misconfiguration-recovery-time .............................................................. 7-394
7.1.54 neighbor-inactivity-timeout ........................................................................ 7-395
7.1.55 neighbor-info-interval ..................................................................................................................7-396
7.1.56 no ...............................................................................................................................................7-397
7.1.57 noc ..............................................................................................................................................7-399
7.1.58 ntp ..............................................................................................................................................7-400
7.1.59 offline-duration .........................................................................................................................7-403
7.1.60 power-config .............................................................................................................................7-404
7.1.61 preferred-controller-group .........................................................................................................7-406
7.1.62 preferred-tunnel-controller .........................................................................................................7-407
7.1.63 radius .........................................................................................................................................7-408
7.1.64 rf-domain-manager ....................................................................................................................7-409
7.1.65 router ..........................................................................................................................................7-410
7.1.66 spanning-tree ..............................................................................................................................7-412
7.1.67 traffic-class-mapping ..................................................................................................................7-415
7.1.68 traffic-shape ................................................................................................................................7-417
7.1.69 trustpoint (profile-config-mode) ...............................................................................................7-422
7.1.70 tunnel-controller .......................................................................................................................7-424
7.1.71 use ................................................................................................................................................7-425
7.1.72 vrrp .............................................................................................................................................7-430
7.1.73 vrrp-state-check ..........................................................................................................................7-434
7.1.74 wep-shared-key-auth ..................................................................................................................7-435
7.1.75 service .........................................................................................................................................7-436
7.1.76 slot ..............................................................................................................................................7-441
7.2.1 adoption-site ................................................................................................................................7-449
7.2.2 area ...............................................................................................................................................7-450
7.2.3 channel-list ..................................................................................................................................7-451
7.2.4 contact ..........................................................................................................................................7-452
7.2.5 country-code ...............................................................................................................................7-453
7.2.6 floor .............................................................................................................................................7-454
7.2.7 geo-coordinates ............................................................................................................................7-455
7.2.8 hostname ....................................................................................................................................7-456
7.2.9 layout-coordinates .......................................................................................................................7-457
7.2.10 license .........................................................................................................................................7-458
7.2.11 location .......................................................................................................................................7-460
7.2.12 mac-name ...................................................................................................................................7-461
7.2.13 no ...............................................................................................................................................7-462
7.2.14 override-wlan .............................................................................................................................7-463
7.2.15 remove-override ..........................................................................................................................7-465
7.2.16 rsa-key .........................................................................................................................................7-467
7.2.17 sensor-server ..............................................................................................................................7-468
7.2.18 timezone ....................................................................................................................................7-469
7.2.19 trustpoint (device-config-mode) ...............................................................................................7-470
7.2.20 mirror .........................................................................................................................................7-472
7.2.21 raid .............................................................................................................................................7-474
7.3.1 cpe ...............................................................................................................................................7-476
7.3.2 interface ........................................................................................................................................7-477
7.3.3 ip ...................................................................................................................................................7-479
7.3.4 no ...............................................................................................................................................7-480
7.3.5 ntp ...............................................................................................................................................7-481
7.3.6 override-wlan .............................................................................................................................7-482
7.3.7 t5 ..................................................................................................................................................7-483
7.3.8 t5-logging ....................................................................................................................................7-484
7.3.9 use ...............................................................................................................................................7-485
7.4.1 interface .......................................................................................................................................7-487
7.4.2 ip ..................................................................................................................................................7-507
7.4.3 power ..........................................................................................................................................7-508
### Chapter 12, DHCP-SERVER-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1.1 bootp</td>
<td>12-4</td>
</tr>
<tr>
<td>12.1.2 dhcp-class</td>
<td>12-5</td>
</tr>
<tr>
<td>12.1.3 dhcp-pool</td>
<td>12-11</td>
</tr>
<tr>
<td>12.1.4 dhcp-server</td>
<td>12-54</td>
</tr>
<tr>
<td>12.1.5 no</td>
<td>12-56</td>
</tr>
<tr>
<td>12.1.6 option</td>
<td>12-57</td>
</tr>
<tr>
<td>12.1.7 ping</td>
<td>12-58</td>
</tr>
<tr>
<td>12.2.1 dhcpv6-pool</td>
<td>12-60</td>
</tr>
<tr>
<td>12.2.2 option</td>
<td>12-71</td>
</tr>
<tr>
<td>12.2.3 restrict-vendor-options</td>
<td>12-73</td>
</tr>
<tr>
<td>12.2.4 server-preference</td>
<td>12-74</td>
</tr>
<tr>
<td>12.2.5 no</td>
<td>12-75</td>
</tr>
</tbody>
</table>

### Chapter 13, FIREWALL-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1.1 acl-logging</td>
<td>13-4</td>
</tr>
<tr>
<td>13.1.2 alg</td>
<td>13-5</td>
</tr>
<tr>
<td>13.1.3 clamp</td>
<td>13-7</td>
</tr>
<tr>
<td>13.1.4 dhcp-offer-convert</td>
<td>13-8</td>
</tr>
<tr>
<td>13.1.5 dns-snoop</td>
<td>13-9</td>
</tr>
<tr>
<td>13.1.6 firewall</td>
<td>13-10</td>
</tr>
<tr>
<td>13.1.7 flow</td>
<td>13-11</td>
</tr>
<tr>
<td>13.1.8 ip</td>
<td>13-13</td>
</tr>
<tr>
<td>13.1.9 ip-mac</td>
<td>13-20</td>
</tr>
<tr>
<td>13.1.10 ipv6</td>
<td>13-23</td>
</tr>
<tr>
<td>13.1.11 ipv6-mac</td>
<td>13-26</td>
</tr>
<tr>
<td>13.1.12 logging</td>
<td>13-28</td>
</tr>
<tr>
<td>13.1.13 no</td>
<td>13-30</td>
</tr>
<tr>
<td>13.1.14 proxy-arp</td>
<td>13-32</td>
</tr>
<tr>
<td>13.1.15 proxy-nd</td>
<td>13-33</td>
</tr>
<tr>
<td>13.1.16 stateful-packet-inspection-12</td>
<td>13-34</td>
</tr>
<tr>
<td>13.1.17 storm-control</td>
<td>13-35</td>
</tr>
<tr>
<td>13.1.18 virtual-defragmentation</td>
<td>13-37</td>
</tr>
</tbody>
</table>

### Chapter 14, MINT-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1.1 level</td>
<td>14-3</td>
</tr>
<tr>
<td>14.1.2 mtu</td>
<td>14-4</td>
</tr>
<tr>
<td>14.1.3 router</td>
<td>14-5</td>
</tr>
<tr>
<td>14.1.4 udp</td>
<td>14-6</td>
</tr>
<tr>
<td>14.1.5 no</td>
<td>14-7</td>
</tr>
</tbody>
</table>

### Chapter 15, MANAGEMENT-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1.1 aaa-login</td>
<td>15-4</td>
</tr>
<tr>
<td>15.1.2 banner</td>
<td>15-6</td>
</tr>
<tr>
<td>15.1.3 ftp</td>
<td>15-7</td>
</tr>
<tr>
<td>15.1.4 http</td>
<td>15-9</td>
</tr>
</tbody>
</table>
# Chapter 16, RADIUS-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1.1 guest</td>
<td>16-4</td>
</tr>
<tr>
<td>16.1.2 policy</td>
<td>16-5</td>
</tr>
<tr>
<td>16.1.3 rate-limit</td>
<td>16-9</td>
</tr>
<tr>
<td>16.1.4 no</td>
<td>16-10</td>
</tr>
<tr>
<td>16.2.1 authentication</td>
<td>16-14</td>
</tr>
<tr>
<td>16.2.2 bypass</td>
<td>16-16</td>
</tr>
<tr>
<td>16.2.3 chase-referral</td>
<td>16-17</td>
</tr>
<tr>
<td>16.2.4 crl-check</td>
<td>16-18</td>
</tr>
<tr>
<td>16.2.5 ldap-agent</td>
<td>16-19</td>
</tr>
<tr>
<td>16.2.6 ldap-group-verification</td>
<td>16-21</td>
</tr>
<tr>
<td>16.2.7 ldap-server</td>
<td>16-22</td>
</tr>
<tr>
<td>16.2.8 local</td>
<td>16-25</td>
</tr>
<tr>
<td>16.2.9 nas</td>
<td>16-26</td>
</tr>
<tr>
<td>16.2.10 no</td>
<td>16-27</td>
</tr>
<tr>
<td>16.2.11 proxy</td>
<td>16-29</td>
</tr>
<tr>
<td>16.2.12 session-resumption</td>
<td>16-31</td>
</tr>
<tr>
<td>16.2.13 termination</td>
<td>16-32</td>
</tr>
<tr>
<td>16.2.14 use</td>
<td>16-33</td>
</tr>
<tr>
<td>16.3.1 duration</td>
<td>16-35</td>
</tr>
<tr>
<td>16.3.2 user</td>
<td>16-36</td>
</tr>
<tr>
<td>16.3.3 no</td>
<td>16-39</td>
</tr>
</tbody>
</table>

# Chapter 17, RADIO-QOS-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1.1 accelerated-multicast</td>
<td>17-5</td>
</tr>
<tr>
<td>17.1.2 admission-control</td>
<td>17-6</td>
</tr>
<tr>
<td>17.1.3 no</td>
<td>17-9</td>
</tr>
<tr>
<td>17.1.4 smart-aggregation</td>
<td>17-11</td>
</tr>
<tr>
<td>17.1.5 service</td>
<td>17-13</td>
</tr>
<tr>
<td>17.1.6 wmm</td>
<td>17-14</td>
</tr>
</tbody>
</table>

# Chapter 18, ROLE-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.1.1 default-role</td>
<td>18-4</td>
</tr>
<tr>
<td>18.1.2 ldap-deadperiod</td>
<td>18-6</td>
</tr>
<tr>
<td>18.1.3 ldap-query</td>
<td>18-7</td>
</tr>
<tr>
<td>18.1.4 ldap-server</td>
<td>18-8</td>
</tr>
<tr>
<td>18.1.5 ldap-timeout</td>
<td>18-10</td>
</tr>
<tr>
<td>18.1.6 no</td>
<td>18-11</td>
</tr>
</tbody>
</table>
Chapter 19, SMART-RF-POLICY

19.1.1 area ......................................................................................................................................................19-4
19.1.2 assignable-power ...................................................................................................................................19-5
19.1.3 avoidance-time .......................................................................................................................................19-6
19.1.4 channel-list ............................................................................................................................................19-8
19.1.5 channel-width ......................................................................................................................................19-9
19.1.6 coverage-hole-recovery ..........................................................................................................................19-11
19.1.7 dfs .........................................................................................................................................................19-13
19.1.8 enable ..................................................................................................................................................19-14
19.1.9 group-by .............................................................................................................................................19-15
19.1.10 interference-recovery ..........................................................................................................................19-16
19.1.11 neighbor-recovery .................................................................................................................................19-18
19.1.12 no .........................................................................................................................................................19-20
19.1.13 sensitivity ..........................................................................................................................................19-22
19.1.14 smart-ocs-monitoring .........................................................................................................................19-23

Chapter 20, WIPS-POLICY

20.1.1 ap-detection .........................................................................................................................................20-5
20.1.2 enable ..................................................................................................................................................20-7
20.1.3 event .....................................................................................................................................................20-8
20.1.4 history-throttle-duration .......................................................................................................................20-12
20.1.5 interference-event ................................................................................................................................20-13
20.1.6 no ..........................................................................................................................................................20-14
20.1.7 signature ............................................................................................................................................20-16
20.1.8 use ......................................................................................................................................................20-32

Chapter 21, WLAN-QOS-POLICY

21.1.1 accelerated-multicast ...........................................................................................................................21-4
21.1.2 classification ......................................................................................................................................21-6
21.1.3 multicast-mask ...................................................................................................................................21-8
21.1.4 no ..........................................................................................................................................................21-9
21.1.5 qos .......................................................................................................................................................21-10
21.1.6 rate-limit .............................................................................................................................................21-11
21.1.7 svp-prioritization .................................................................................................................................21-14
21.1.8 voice-prioritization ...............................................................................................................................21-15
21.1.9 wmm ..................................................................................................................................................21-16

Chapter 22, L2TPV3-POLICY

22.1.1 cookie-size ..........................................................................................................................................22-5
22.1.2 failover-delay ......................................................................................................................................22-6
22.1.3 force-l2-path-recovery ..........................................................................................................................22-7
22.1.4 hello-interval .....................................................................................................................................22-8
22.1.5 no ..........................................................................................................................................................22-9
22.1.6 reconnect-attempts ...............................................................................................................................22-10
22.1.7 reconnect-interval .................................................................................................................................22-11
22.1.8 retry-attempts ...................................................................................................................................22-12
22.1.9 retry-interval .....................................................................................................................................22-13
22.1.10 rx-window-size .................................................................................................................................22-14
Chapter 27, PASSPOINT POLICY

27.1.1 3gpp ................................................................................................................................. 27-4
27.1.2 access-network-type ....................................................................................................... 27-5
27.1.3 connection-capability .................................................................................................... 27-6
27.1.4 domain-name .................................................................................................................. 27-7
27.1.5 hessid .............................................................................................................................. 27-8
27.1.6 internet ............................................................................................................................. 27-9
27.1.7 ip-address-type .............................................................................................................. 27-10
27.1.8 nai-realm ....................................................................................................................... 27-11
27.1.9 net-auth-type .................................................................................................................. 27-12
27.1.10 no ................................................................................................................................. 27-13
27.1.11 operator ......................................................................................................................... 27-14
27.1.12 osu ................................................................................................................................ 27-15
27.1.13 roam-consortium ......................................................................................................... 27-16
27.1.14 venue ............................................................................................................................ 27-17
27.1.15 wan-metrics .................................................................................................................. 27-18

Chapter 28, BORDER GATEWAY PROTOCOL

28.1.1 deny .................................................................................................................................. 28-4
28.1.2 permit ............................................................................................................................... 28-5
28.1.3 no ...................................................................................................................................... 28-6
28.2.1 deny ................................................................................................................................. 28-7
28.2.2 permit ............................................................................................................................... 28-8
28.2.3 no ...................................................................................................................................... 28-9
28.3.1 deny .................................................................................................................................. 28-10
28.3.2 permit ............................................................................................................................... 28-11
28.3.3 no ...................................................................................................................................... 28-12
28.4.1 deny .................................................................................................................................. 28-13
28.4.2 permit ............................................................................................................................... 28-14
28.4.3 no ...................................................................................................................................... 28-15
28.5.1 deny .................................................................................................................................. 28-16
28.5.2 permit ............................................................................................................................... 28-17
Chapter 30, ROAMING ASSIST POLICY

30.1.1 action .......................................................................................................................... 30-4
30.1.2 aggressiveness ........................................................................................................... 30-5
30.1.3 detection-threshold .................................................................................................. 30-6
30.1.4 disassoc-time .......................................................................................................... 30-7
30.1.5 handoff-count ........................................................................................................ 30-8
30.1.6 handoff-threshold .................................................................................................. 30-9
30.1.7 monitoring-interval ............................................................................................... 30-10
30.1.8 sampling-interval ................................................................................................. 30-11
30.1.9 no .......................................................................................................................... 30-12

Appendix A, CONTROLLER MANAGED WLAN USE CASE

A.1.1 Assumptions .............................................................................................................. A-2
A.1.2 Design .................................................................................................................. A-2
A.1.3 Using the Command Line Interface to Configure the WLAN ......................... A-3

Appendix B, PUBLICLY AVAILABLE SOFTWARE

B.3.1 Apache License, Version 2.0 ................................................................................ B-10
B.3.2 The BSD License .................................................................................................. B-12
B.3.3 Creative Commons Attribution-ShareAlike License, version 3.0 ...................... B-12
B.3.4 DropBear License ............................................................................................... B-16
B.3.5 GNU General Public License, version 2 ................................................................ B-18
B.3.6 GNU Lesser General Public License 2.1 ............................................................ B-22
B.3.7 GNU General Public License, version 3 .............................................................. B-27
B.3.8 ISC License .......................................................................................................... B-35
B.3.9 GNU Lesser General Public License, version 3 ................................................ B-35
B.3.10 GNU General Public License 2.0 ......................................................................... B-37
B.3.11 GNU Lesser General Public License, version 2.0 ............................................. B-42
B.3.12 GNU Lesser General Public License, version 2.1 ............................................. B-47
B.3.13 MIT License ...................................................................................................... B-52
B.3.14 Mozilla Public License, version 2 ....................................................................... B-52
B.3.15 The Open LDAP Public License ................................................................. B-56
B.3.16 OpenSSL License .............................................................................................. B-57
B.3.17 WU-FTPD Software License ............................................................................... B-57
B.3.18 zlib License ....................................................................................................... B-59

Appendix C, CUSTOMER SUPPORT
This manual supports the following wireless controllers, service platforms, and access points:

- **Wireless Controllers** – RFS4000, RFS6000, RFS7000
- **Service Platforms** – NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600
- **Access Points** – AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP7131, AP7161, AP7181, AP7502, AP7522, AP7532, AP7562, AP8122, AP8132, AP8163, AP8222, AP8232

---

**NOTE:** ES6510 is an *Ethernet Switch* managed by a wireless controller or service platform, such as RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, and NX9600. ES6510 does not have radios and does not provide WLAN support.

---

**NOTE:** In this guide,

- AP7131, AP7161, and AP7181 are collectively represented as AP71XX.
- AP8122, AP8132, and AP8163 are collectively represented as AP81XX. AP8163 is an outdoor mesh supporting access point.
- AP8222 and AP8232 are collectively represented as AP82XX.
- NX4500 and NX4524 are collectively represented as NX45XX.
- NX6500 and NX6524 are collectively represented as NX65XX.
- NX7510, NX7520, and NX7530 are collectively represented as NX7500 series.
- NX9000, NX9500, and NX9510 are collectively represented as NX9000 series.

---

A simplified version of the WiNG operating system *user interface* (UI) is available on the following access point and service platform models with the E-SKU:

- AP6511, AP6521, AP6522, AP6562, AP7502, AP7522, AP7532, and AP7562
- NX7510

This new UI, referred to as the WiNG *Express* (WE) UI, simplifies configuration and monitoring of small access point deployments by limiting monitoring, analytics, and configuration capabilities. The WE UI is designed for single-site access point deployments not exceeding more than 24 access points of the same model.
CAUTION: If using the WiNG Express (WE) UI, to configure a WE access point, use the WE UI exclusively. Do not use the command line interface (CLI) along with it. Similarly, when using the CLI to configure the WE access point, do not use the WE UI along with it.

This section is organized into the following topics:

- Document Conventions
- Notational Conventions
- End-User Software License Agreement
Document Conventions

The following conventions are used in this document to draw your attention to important information:

**NOTE:** Indicates tips or special requirements.

---

**CAUTION:** Indicates conditions that can cause equipment damage or data loss.

---

**WARNING!** Indicates a condition or procedure that could result in personal injury or equipment damage.

---

**Switch Note:** Indicates caveats unique to a RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, or NX9600 model controller.
Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
- Bullets (∗) indicate:
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
  - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

Understanding Command Syntax

| <variable> | Variables are described with a short description enclosed within a '<' and a '>' pair.  
For example, the command,  
```
show interface ge 1
```

where:  
- show – is the command – displays information  
- interface – is the keyword – represents the interface type  
- <1-4> – is the variable – represents the ge interface index value |

|  | The pipe symbol. This is used to separate the variables/keywords in a list.  
For example, the command,  
```
rfs7000-37FABE>show adoption|bonjour|boot
```

where:
- show – is the command – displays information  
- [adoption|bonjour|......] – indicates the different keywords that can be combined with the show command. However, only one of the above option can be used at a time.
Of the different keywords and variables listed inside a `[]` pair, only one can be used. Each choice in the list is separated with a `|` (pipe) symbol. For example, the command,

```
rfs7000-37FABE#clear ...
```

is documented as:

```
clear [arp-cache|bonjour|cdp|counters|crypto|
  event-history|firewall|gre|ip|ipv6|
  l2tpv3-stats|license|lldp|logging|
  mac-address-table|mint|role|rtls|
  spanning-tree|traffic-shape|vrrp]
```

where:
- `clear` – is the command
- `[arp-cache|cdp|counters|crypto|event-history|firewall|gre|ip|ipv6|
  l2tpv3-stats|license|lldp|logging|
  mac-address-table|mint|role|rtls|
  spanning-tree|traffic-shape|vrrp]` – indicates that these keywords are available for this command. However, only one can be used at a time.

Any command/keywordvariable or a combination of them inside a `{ }` pair is optional. All optional commands follow the same conventions as listed above. However, they are displayed italicized.

For example, the command,

```
rfs7000-37FABE> show adoption ....
```

is documented as:

```
show adoption info {on <DEVICE-NAME>}
```

here:
- `show adoption info` – is the command. This command can also be used as:
  ```
  show adoption info
  ```

The command can also be extended as:

```
show adoption info {on <DEVICE-NAME>}
```

here:
- `{on <DEVICE-NAME>}` – is the keyword, which is optional.

The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.

For example, the command,

```
rfs7000-37FABE> show wireless
```

is documented as:

```
show wireless
```

where:
- `show` – is the command
- `wireless` – is the keyword
Any command/keyword-variable or a combination of them inside a '()' pair are recursive. All recursive commands can be listed in any order and can be used once along with the rest of the commands.

For example, the command,

```plaintext
crypto pki export request generate-rsa-key
test autogen-subject-name ...
```

is documented as:

```plaintext
rfs7000-37FABE#crypto pki export request
generate-rsa-key test autogen-subject-name
(<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>)
```

here:

- crypto pki export request generate-rsa-key <RSA-KEYPAIR-NAME> auto-gen-subject-name – is the command
- <RSA-KEYPAIR-NAME> – is the RSA keypair name (in this example, the keypair name is ‘test’), and is a variable
- (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>) – is the set of recursive parameters (separated by commas) that can be used in any order.
End-User Software License Agreement

BY INSTALLING AND/OR USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, ZEBRA IS NOT WILLING TO LICENSE THE PRODUCT TO YOU, AND YOU MUST NOT INSTALL OR USE THIS PRODUCT.

GRANT OF LICENSE. Zebra Technologies Corporation ("Zebra") grants you ("Licensee" or "you") a personal, nonexclusive, nontransferable, revocable, nonassignable, limited license to use the software and documentation ("Product(s)") subject to the terms and conditions of this Agreement. You shall use the Products only for your internal business purposes, exclusively to support Zebra devices. Any use of the Products outside of the conditions set forth herein is strictly prohibited and will be deemed a breach of this Agreement resulting in immediate termination of your License. In the event of a breach of this Agreement, Zebra will be entitled to all available remedies at law or in equity (including immediate immediate termination of the license without notice, immediate injunctive relief and repossess of all Products unless Licensee is a Federal agency of the United States Government).

You shall not distribute, sublicense, rent, loan, lease, export, re-export, resell, ship or divert or cause to be exported, re-exported, resold, shipped or diverted, directly or indirectly, the Products under this Agreement. You shall not, and shall not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or the inner workings of the Products, (ii) copy the look-and-feel or functionality of the Products; (iii) remove any proprietary notices, marks, labels, or logos from the Products; (iv) rent or transfer all or some of the Products to any other party without Zebra’s prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Products be equipped with such a protection device.

Title to all copies of Products will not pass to Licensee at any time and remains vested exclusively in Zebra. All intellectual property developed, originated, or prepared by Zebra in connection with the Products remain vested exclusively in Zebra, and this Agreement does not grant to Licensee any intellectual property rights.

Portions of the Products are protected by United States patent and copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Products like any other copyrighted material (e.g., a book or musical recording) except that you may make one copy of the Product solely for back-up purposes. Unauthorized duplication of the Products constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

LIMITED WARRANTY. Zebra warrants for a period of ninety (90) days from your receipt of the Products to you that the Software, under normal use, will perform substantially in accordance with Zebra’s published specifications for that release level of the Software. The written materials are provided “AS IS” and without warranty of any kind. Zebra’s entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Zebra’s option, the provision of a downloadable patch or replacement code, or a refund of the unused portion of your bargained for contractual benefit up to the amount paid for the Products.

DISCLAIMER. THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY ZEBRA, AND ZEBRA MAKES, AND YOU RECEIVE, NO OTHER WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. ZEBRA SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. ZEBRA DOES NOT WARRANT THAT THE PRODUCTS WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE PRODUCTS WILL BE CORRECTED. ZEBRA MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE PRODUCTS. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

LIMITATION OF LIABILITY. THE TOTAL LIABILITY OF ZEBRA UNDER THIS AGREEMENT FOR DAMAGES SHALL NOT EXCEED THE FAIR MARKET VALUE OF THE PRODUCTS LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL ZEBRA BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER ZEBRA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you. This Limitation of Liability provision survives the termination of this Agreement.
and applies notwithstanding any contrary provision in this Agreement. Licensee must bring any action under this Agreement within one (1) year after the cause of action arises.

MAINTENANCE. Unless provided for in a separate agreement, Zebra shall not be responsible for maintenance or field service of the Products.

HIGH RISK ACTIVITIES. The Products are not fault-tolerant and are not designed, manufactured or intended for use or resale as on-line control software in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Products could lead directly to death, personal injury, or severe physical or environmental damage (“High Risk Activities”).

Zebra and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities, and if you elect to use the Products in any High Risk Activities, you agree to indemnify, defend, and hold Zebra harmless from and against any and all costs, damages, and losses related to that use.

U.S. GOVERNMENT. If you are acquiring the Products on behalf of any unit or agency of the U.S. Government, the following shall apply. Use, duplication, or disclosure of the Products is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Products may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement shall each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

ASSIGNMENT. Except as otherwise provided in this section, neither party may assign this Agreement, or any of its rights or obligations under this Agreement, without the prior written approval of the other party, which will not be unreasonably withheld. Any attempted assignment, delegation, or transfer without the necessary approval will be void. Notwithstanding the foregoing, for any Zebra acquisition, merger, consolidation, reorganization, or similar transaction, or any spin-off, divestiture, or other separation of a Zebra business, Zebra may, without the prior written consent of the other party: (i) assign its rights and obligations under this Agreement, in whole or in part, or (ii) split and assign its rights and obligations under this Agreement so as to retain the benefits of this Agreement for both Zebra and the assignee entity(ies) (and their respective Affiliates) following the split.

GOVERNING LAW. This Agreement shall be governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of New York without regard to its conflict of laws provisions or by the internal substantive laws of the country to which the Products is shipped if end-user customer is a sovereign governmental entity. The terms of the U.N. Convention on Contracts for the International Sale of Goods do not apply. In the event that the Uniform Computer information Transaction Act, any version of this Act, or a substantially similar law (collectively “UCITA”) becomes applicable to a Party’s performance under this Agreement, UCITA does not govern any aspect of this End User License Agreement or any license granted under this End-User License Agreement, or any of the parties’ rights or obligations under this End User License Agreement. The governing law will be that in effect prior to the applicability of UCITA.

COMPLIANCE WITH LAWS. Licensee will comply with all applicable laws and regulations, including export laws and regulations of the United States. Licensee will not, without the prior authorization of Zebra and the appropriate governmental authority of the United States, in any form export or re-export, sell or resell, ship or reship, or divert, through direct or indirect means, any item or technical data or direct or indirect products sold or otherwise furnished to any person within any territory for which the United States Government or any of its agencies at the time of the action, requires an export license or other governmental approval. Violation of this provision will be a material breach of this Agreement, permitting immediate termination by Zebra.

THIRD PARTY SOFTWARE. The Products may contain one or more items of Third-Party Software. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.
OPEN SOURCE SOFTWARE. The Products may contain one or more items of Open Source Software. Open Source Software is software covered by a publicly available license governed solely under Copyright law, whereas the complete terms and obligations of such license attach to a licensee solely through the act of copying, using and/or distribution of the licensed software, such obligations often include one or more of attribution obligations, distribution obligations, copyleft obligations, and intellectual property encumbrances. The use of any Open Source Software is subject to the terms and conditions of this Agreement as well as the terms and conditions of the corresponding license of each Open Source Software package. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the Open Source Software license, the applicable Open Source Software license will take precedence. Copies of the licenses for the included Open Source Software, if any, as well as their attributions, acknowledgements, and software information details, are provided in the electronic copy of this Agreement, which is available in the Legal Notices or README file associated with the Product. Zebra is required to reproduce the software licenses, acknowledgments and copyright notices as provided by the authors and owners, thus, all such information is provided in its native language form, without modification or translation. Depending on the license terms of the specific Open Source Software, source code may not be provided. Please reference and review the entire Open Source Software information to identify which Open Source Software packages have source code provided or available. For instructions on how to obtain a copy of any source code made publicly available by Zebra related to Open Source Software distributed by Zebra, you may send your request (including the Zebra Product name and version, along with the Open Source Software specifics) in writing to: Zebra Technologies Corporation, Open Source Software Director, Legal Department, 3 Overlook Point, Lincolnshire, IL 60069 USA.

©2015 ZIH Corp and/or its affiliates. All rights reserved. Zebra and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.
This chapter describes the commands available within a device’s Command Line Interface (CLI) structure. CLI is available for wireless controllers, access points (APs), and service platforms.

Access the CLI by using:
- A terminal emulation program running on a computer connected to the serial port on the device (access point, wireless controller, and service platform).
- A Telnet session through Secure Shell (SSH) over a network.

**Configuration for connecting to a Controller using a terminal emulator**

If connecting through the serial port, use the following settings to configure your terminal emulator:

<table>
<thead>
<tr>
<th>Bits Per Second</th>
<th>19200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop Bit</td>
<td>1</td>
</tr>
<tr>
<td>Flow Control</td>
<td>None</td>
</tr>
</tbody>
</table>

When a CLI session is established, complete the following (user input is in **bold**):

login as: **<username>**
administrator’s login password: **<password>**

**User Credentials**

Use the following credentials when logging into a device for the first time:

<table>
<thead>
<tr>
<th>User Name</th>
<th>admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>admin123</td>
</tr>
</tbody>
</table>

When logging into the CLI for the first time, you are prompted to change the password.
Examples in this reference guide
Examples used in this reference guide are generic to each supported wireless controller, service platform, and AP model. Commands that are not common, are identified using the notation “Supported in the following platforms:” For an example, see below:

Supported in the following platforms:
• Wireless Controller – RFS6000

The above example indicates the command is only available for a RFS6000 model wireless controller.

This chapter is organized into the following sections:
• CLI Overview
• Getting Context Sensitive Help
• Using the No Command
• Using CLI Editing Features and Shortcuts
• Using CLI to Create Profiles and Enable Remote Administration

1.1 CLI Overview

INTRODUCTION

The CLI is used for configuring, monitoring, and maintaining the network. The user interface allows you to execute commands on supported wireless controllers, service platforms, and APs, using either a serial console or a remote access method.

This chapter describes basic CLI features. Topics covered include an introduction to command modes, navigation and editing features, help features and command history.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance, and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular model used. Enter a question mark (?) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

![Hierarchy of User Modes](image-url)
Command Modes

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the device’s (wireless controller, service platform, or AP) configuration.

```
rfs7000-37FABE>
```

The system prompt signifies the device name and the last three bytes of the device MAC address.

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

```
rfs7000-37FABE>enable
rfs7000-37FABE#
```

Most of the USER EXEC mode commands are one-time commands and are not saved across device reboots. Save the command by executing `commit` command. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In the GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across device reboots.

Access a variety of protocol specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you to access specific configuration modes only through the global configuration mode.

```
rfs7000-37FABE#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs7000-37FABE(config)#
```

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

```
rfs7000-37FABE(config)#aaa-policy test
rfs7000-37FABE(config-aaa-policy-test)#
```

The following table summarizes available CLI commands:

<table>
<thead>
<tr>
<th>User Exec Mode</th>
<th>Priv Exec Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal-page-upload</td>
<td>archive</td>
<td>aaa-policy</td>
</tr>
<tr>
<td>change-passwd</td>
<td>boot</td>
<td>aaa-tacacs-policy</td>
</tr>
<tr>
<td>clear</td>
<td>captive-portal-page-upload</td>
<td>alias</td>
</tr>
<tr>
<td>clock</td>
<td>cd</td>
<td>ap621</td>
</tr>
<tr>
<td>cluster</td>
<td>change-passwd</td>
<td>ap622</td>
</tr>
<tr>
<td>commit</td>
<td>clear</td>
<td>ap650</td>
</tr>
<tr>
<td>connect</td>
<td>clock</td>
<td>ap6511</td>
</tr>
<tr>
<td>create-cluster</td>
<td>cluster</td>
<td>ap6521</td>
</tr>
<tr>
<td>crypto</td>
<td>commit</td>
<td>ap6522</td>
</tr>
<tr>
<td>crypto-cmp-cert-update</td>
<td>configure</td>
<td>ap6532</td>
</tr>
<tr>
<td>database</td>
<td>connect</td>
<td>ap6562</td>
</tr>
<tr>
<td>database-backup</td>
<td>copy</td>
<td>ap71XX</td>
</tr>
<tr>
<td>database-restore</td>
<td>create-cluster</td>
<td>ap7502</td>
</tr>
<tr>
<td>debug</td>
<td>crypto</td>
<td>ap7522</td>
</tr>
</tbody>
</table>

The following table summarizes available CLI commands:

Table 1.1 Controller CLI Modes and Commands
### Table 1.1 Controller CLI Modes and Commands

<table>
<thead>
<tr>
<th>User Exec Mode</th>
<th>Priv Exec Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>device-upgrade</td>
<td>crypto-cmp-cert-update</td>
<td>ap7532</td>
</tr>
<tr>
<td>disable</td>
<td>database</td>
<td>ap7562</td>
</tr>
<tr>
<td>enable</td>
<td>database-backup</td>
<td>ap81xx</td>
</tr>
<tr>
<td>file-sync</td>
<td>database-restore</td>
<td>ap82xx</td>
</tr>
<tr>
<td>help</td>
<td>debug</td>
<td>application</td>
</tr>
<tr>
<td>join-cluster</td>
<td>delete</td>
<td>application-policy</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>device-upgrade</td>
<td>association-acl-policy</td>
</tr>
<tr>
<td>logging</td>
<td>diff</td>
<td>auto-provisioning-policy</td>
</tr>
<tr>
<td>mint</td>
<td>dir</td>
<td>bgp</td>
</tr>
<tr>
<td>no</td>
<td>disable</td>
<td>bonjour-gw-discovery-policy</td>
</tr>
<tr>
<td>on</td>
<td>edit</td>
<td>bonjour-gw-forwarding-policy</td>
</tr>
<tr>
<td>opensd</td>
<td>enable</td>
<td>bonjour-gw-query-forwarding-policy</td>
</tr>
<tr>
<td>page</td>
<td>erase</td>
<td>captive-portal</td>
</tr>
<tr>
<td>ping</td>
<td>ex3500</td>
<td>clear</td>
</tr>
<tr>
<td>ping6</td>
<td>factory-reset</td>
<td>client-identity</td>
</tr>
<tr>
<td>revert</td>
<td>file-sync</td>
<td>client-identity-group</td>
</tr>
<tr>
<td>service</td>
<td>halt</td>
<td>clone</td>
</tr>
<tr>
<td>show</td>
<td>help</td>
<td>crypto-cmp-policy</td>
</tr>
<tr>
<td>ssh</td>
<td>join-cluster</td>
<td>customize</td>
</tr>
<tr>
<td>telnet</td>
<td>l2tpv3</td>
<td>device</td>
</tr>
<tr>
<td>terminal</td>
<td>logging</td>
<td>device-categorization</td>
</tr>
<tr>
<td>time-it</td>
<td>mint</td>
<td>dhcp-server-policy</td>
</tr>
<tr>
<td>traceroute</td>
<td>mkdir</td>
<td>dhcp6-server-policy</td>
</tr>
<tr>
<td>traceroute6</td>
<td>more</td>
<td>dns-whitelist</td>
</tr>
<tr>
<td>watch</td>
<td>no</td>
<td>event-system-policy</td>
</tr>
<tr>
<td>write</td>
<td>on</td>
<td>ex3500</td>
</tr>
<tr>
<td>clrschr</td>
<td>opensd</td>
<td>ex3500-management-policy</td>
</tr>
<tr>
<td>exit</td>
<td>page</td>
<td>ex3500-qos-class-map-policy</td>
</tr>
<tr>
<td>smart-cache (NX45XX, NX65XX, NX9XXX)</td>
<td>ping</td>
<td>ex3500-qos-policy-map</td>
</tr>
<tr>
<td>User Exec Mode</td>
<td>Priv Exec Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>virtual-machine (NX45XX, NX65XX, NX9XXX)</td>
<td>ping6</td>
<td>ex3524</td>
</tr>
<tr>
<td></td>
<td>pwd</td>
<td>ex3548</td>
</tr>
<tr>
<td></td>
<td>re-elect</td>
<td>firewall-policy</td>
</tr>
<tr>
<td></td>
<td>reload</td>
<td>global-association-list</td>
</tr>
<tr>
<td></td>
<td>remote-debug</td>
<td>guest-management</td>
</tr>
<tr>
<td></td>
<td>rename</td>
<td>help</td>
</tr>
<tr>
<td></td>
<td>revert</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>rmdir</td>
<td>igmp-snoop-policy (This command has been deprecated. IGMP snooping is now configurable under the profile/device configuration mode. For more information, see ip.)</td>
</tr>
<tr>
<td></td>
<td>self</td>
<td>inline-password-encryption</td>
</tr>
<tr>
<td></td>
<td>service</td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>show</td>
<td>ipv6</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>ipv6-router-advertisement-policy</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>l2tpv3</td>
</tr>
<tr>
<td></td>
<td>terminal</td>
<td>mac</td>
</tr>
<tr>
<td></td>
<td>time-it</td>
<td>management-policy</td>
</tr>
<tr>
<td></td>
<td>traceroute</td>
<td>meshpoint</td>
</tr>
<tr>
<td></td>
<td>traceroute6</td>
<td>meshpoint-qos-policy</td>
</tr>
<tr>
<td></td>
<td>upgrade</td>
<td>mint-policy</td>
</tr>
<tr>
<td></td>
<td>upgrade-abort</td>
<td>nac-list</td>
</tr>
<tr>
<td></td>
<td>watch</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>write</td>
<td>nsight-policy</td>
</tr>
<tr>
<td></td>
<td>clrscrm</td>
<td>passpoint-policy</td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>password-encryption</td>
</tr>
<tr>
<td></td>
<td>smart-cache (NX45XX, NX65XX, NX9XXX)</td>
<td>profile</td>
</tr>
<tr>
<td></td>
<td>virtual-machine (NX45XX, NX65XX, NX9XXX)</td>
<td>radio-qos-policy</td>
</tr>
<tr>
<td></td>
<td>raid (NX9500, NX7530)</td>
<td>radius-group</td>
</tr>
<tr>
<td>User Exec Mode</td>
<td>Priv Exec Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>cpe (RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX9XXX)</td>
<td>radius-server-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>radius-user-pool-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rename</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rf-domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rfs4000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rfs6000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rfs7000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx45xx series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx5500</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx65xx series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx75xx series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx9000 series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx9600</td>
<td></td>
</tr>
<tr>
<td></td>
<td>role-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>roaming-assist-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>route-map</td>
<td></td>
</tr>
<tr>
<td></td>
<td>routing-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>self</td>
<td></td>
</tr>
<tr>
<td></td>
<td>smart-rf-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wips-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wlan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wlan-qos-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>write</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clrscr</td>
<td></td>
</tr>
<tr>
<td></td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>do</td>
<td></td>
</tr>
<tr>
<td></td>
<td>end</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>revert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show</td>
<td></td>
</tr>
</tbody>
</table>

*Table 1.1 Controller CLI Modes and Commands*
### Table 1.1 Controller CLI Modes and Commands

<table>
<thead>
<tr>
<th>User Exec Mode</th>
<th>Priv Exec Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>smart-cache-policy (NX45XX, NX65XX, and NX9XXX)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>url-filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>url-list (NX45XX, NX65XX, and NX9XXX)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vx9000 (NX9000)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>web-filter-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>t5 (RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX9XXX)</td>
</tr>
</tbody>
</table>
1.2 Getting Context Sensitive Help

INTRODUCTION

Enter a question mark (?) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(prompt)#help</td>
<td>Displays a brief description of the help system</td>
</tr>
<tr>
<td>(prompt)#abbreviated-command-entry?</td>
<td>Lists commands in the current mode that begin with a particular character string</td>
</tr>
<tr>
<td>(prompt)#abbreviated-command-entry[TAB]</td>
<td>Completes a partial command name</td>
</tr>
<tr>
<td>(prompt)#?</td>
<td>Lists all commands available in the command mode</td>
</tr>
<tr>
<td>(prompt)#command ?</td>
<td>Lists the available syntax options (arguments and keywords) for the command</td>
</tr>
<tr>
<td>(prompt)#command keyword ?</td>
<td>Lists the next available syntax option for the command</td>
</tr>
</tbody>
</table>

NOTE: The system prompt varies depending on the configuration mode.

NOTE: Enter Ctrl + V to use ? as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a ?

NOTE: The escape character used throughout the CLI is \"\". To enter a "\" use "\\" instead.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called word help, because it completes a word.

rfs7000-37FABE#service?
service Service Commands
rfs7000-37FABE#service
Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the “?” . This form of help is called command syntax help. It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
rfs7000-37FABE#service ?
    block-adopter-config-update       Block configuration updates from the adopter
    clear                             Clear adoption history
    cli-tables-skin                   Choose a formatting layout/skin for CLI tabular outputs
    cluster                           Cluster Protocol
    copy                               Copy from one file to another
    delete                            Delete sessions
    delete-offline-aps                Delete Access Points that are configured but offline
    force-send-config                 Resend configuration to the device
    force-update-vm-stats             Force VM statistics to be pushed up to the NOC
    load-balancing                    Wireless load-balancing service commands
    locator                           Enable leds flashing on the device
    mint                              MiNT protocol
    pktcap                            Start packet capture
    pm                                Process Monitor
    radio                             Radio parameters
    radius                            Radius test
    request-full-config-from-adopter  Request full configuration from the adopter
    set                               Set validation mode
    show                              Show running system information
    signal                            Send a signal to a process
    smart-rf                          Smart-RF Management Commands
    snmp                              Snmp
    ssm                               Command related to ssm
    start-shell                       Provide shell access
    syslog                            Test the syslog server configuration
    trace                             Trace a process for system calls and signals
    wireless                          Command related to wireless
```

It is possible to abbreviate commands and keywords to allow a unique abbreviation. For example, "configure terminal" can be abbreviated as config t. Since the abbreviated command is unique, the controller accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
rfs7000-37FABE#help
```

When using the CLI, help is provided at the command line when typing ' ?'.

If no help is available, the help content will be empty. Backup until entering a '?' shows the help content.

There are two styles of help provided:

1. Full help. Available when entering a command argument (e.g. 'show ?'). This will describe each possible argument.

2. Partial help. Available when an abbreviated argument is entered. This will display which arguments match the input (e.g. 'show ve?').

```
rfs7000-37FABE>
```
1.3 Using the No Command

INTRODUCTION
Almost every command has a no form. Use no to disable a feature or function or return it to its default. Use the command without the no keyword to re-enable a disabled feature.

1.3.1 Basic Conventions
Keep the following conventions in mind while working within the CLI structure:
• Use ? at the end of a command to display available sub-modes. Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using ? until you reach the last sub-mode.
• Pre-defined CLI commands and keywords are case-insensitive: cfg = Cfg = CFG. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, apPolicy, trapHosts, channelInfo.
• Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

1.4 Using CLI Editing Features and Shortcuts

INTRODUCTION
A variety of shortcuts and edit features are available. The following sections describe these features:
• Moving the Cursor on the Command Line
• Completing a Partial Command Name
• Command Output Pagination

1.4.1 Moving the Cursor on the Command Line

Using CLI Editing Features and Shortcuts
The following table shows the key combinations or sequences to move the command line cursor. Ctrl defines the control key, which must be pressed simultaneously with its associated letter key. Esc means the escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions.

Table 1.2 Keystrokes Details

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Function Summary</th>
<th>Function Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left Arrow</td>
<td>Back character</td>
<td>Moves the cursor one character to the left</td>
</tr>
<tr>
<td>or Ctrl-B</td>
<td></td>
<td>When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to move back to the system prompt.</td>
</tr>
<tr>
<td>Right Arrow or Ctrl-F</td>
<td>Forward character</td>
<td>Moves the cursor one character to the right</td>
</tr>
<tr>
<td>Esc- B</td>
<td>Back word</td>
<td>Moves the cursor back one word</td>
</tr>
<tr>
<td>Esc- F</td>
<td>Forward word</td>
<td>Moves the cursor forward one word</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Beginning of line</td>
<td>Moves the cursor to the beginning of the command line</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>End of line</td>
<td>Moves the cursor to the end of the command line</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td></td>
<td>Deletes the current character</td>
</tr>
<tr>
<td>Ctrl-U</td>
<td></td>
<td>Deletes text up to cursor</td>
</tr>
</tbody>
</table>
1.4.2 Completing a Partial Command Name

Using CLI Editing Features and Shortcuts

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform), enter the first few letters of a command, then press the Tab key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-L.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter "conf" within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with conf.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
rfs7000-37FABE#conf[TAB]
rfs7000-37FABE#configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the Return or Enter key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering U lists all commands available in the current command mode:

```
rfs7000-37FABE#cc?
commit     Commit all changes made in this session
configure  Enter configuration mode
connect    Open a console connection to a remote device
copy       Copy from one file to another
```

faithful: The characters entered before the question mark are reprinted to the screen to complete the command entry.
1.4.3 Command Output Pagination

Using CLI Editing Features and Shortcuts

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a `--More--` prompt displays at the bottom of the screen. To resume the output, press the Enter key to scroll down one line or press the Spacebar to display the next full screen of output.

1.5 Using CLI to Create Profiles and Enable Remote Administration

INTRODUCTION

The following sections describe the following essential procedures:

- Creating Profiles
- Changing the default profile by creating vlan 150 and mapping to ge3 Physical interface
- Enabling Remote Administration

1.5.1 Creating Profiles

Using CLI to Create Profiles and Enable Remote Administration

Profiles are sort of a ‘template’ representation of configuration. The system has:

- a default profile for each of the following devices:
  - RFS4000, RFS6000, RFS7000
- a default profile for each of the following service platforms:
  - NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600
- a default profile for each of the following access points:
  - AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX

To modify the default profile to assign an IP address to the management port:

```
rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#interface me1
rfs7000-37FABE(config-profile-default-rfs7000-if-me1)#ip address 172.16.10.2/24
rfs7000-37FABE(config-profile-default-rfs7000-if-me1)#commit
rfs7000-37FABE(config-profile-default-rfs7000)#exit
```

The following command displays a default AP71XX profile:

```
rfs7000-37FABE(config)#profile ap71xx default-ap71xx
rfs7000-37FABE(config-profile-default-ap71xx)#
rfs7000-37FABE(config-profile-default-ap71xx)#show context
profile ap71xx default-ap71xx
autoinstall configuration
autoinstall firmware
device-upgrade persist-images
crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radio1
```
interface radio2
interface radio3
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp

--More--

1.5.2 Changing the default profile by creating vlan 150 and mapping to ge3

Physical interface

Using CLI to Create Profiles and Enable Remote Administration

Logon to the controller in config mode and follow the procedure below:

rfs7000-37FABE(config-profile-default-rfs7000)#interface vlan 150
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan150)#ip address 192.168.150.20/24
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan150)#exit
rfs7000-37FABE(config-profile-default-rfs7000)#interface ge 3
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)#switchport access vlan 150
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)#commit write
[OK]
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)#show interface vlan 150

Interface vlan150 is UP
Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
Index: 8, Metric: 1, MTU: 1500
IP-Address: 192.168.150.20/24
input packets 43, bytes 12828, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 0, bytes 0, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0

1.5.2.1 Viewing Configured APs

To view previously configured APs, enter the following command:

rfs7000-6DCD4B#show wireless ap configured

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap7131-11E6C4</td>
<td>00-23-68-11-B6-C4</td>
<td>default-ap71xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap8132-711728</td>
<td>B4-C7-99-71-17-28</td>
<td>default-ap81xx</td>
<td>00-15-70-81-74-2D</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ap81xx-74B45C</td>
<td>B4-C7-99-74-B4-5C</td>
<td>default-ap81xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B#

1.5.3 Enabling Remote Administration

Using CLI to Create Profiles and Enable Remote Administration

A terminal server may function in remote administration mode if either the terminal services role is not installed on
the machine or the client used to invoke the session has enabled the admin controller.

• A terminal emulation program running on a computer connected to the serial port on the controller. The serial
port is located on the front of the controller.

• A Telnet session through a Secure Shell (SSH) over a network. The Telnet session may or may not use SSH
depending on how the controller is configured. It is recommended you use SSH for remote administration tasks.

This section is organized into the following sub sections:

• Configuring Telnet for Management Access
• Configuring SSH
1.5.3.1 Configuring Telnet for Management Access

**Enabling Remote Administration**

Login through the serial console. Perform the following:

1. A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode).

2. Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

   ```
   rfs7000-37FABE>en
   rfs7000-37FABE#configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
   ```

3. Go to ‘default-management-policy’ mode.

   ```
   rfs7000-37FABE(config)#management-policy ?
   rfs7000-37FABE(config)#management-policy default
   rfs7000-37FABE(config-management-policy-default)#
   ```

4. Enter Telnet and the port number at the command prompt. The port number is optional. The default port is 23. Commit the changes after every command. Telnet is enabled.

   ```
   rfs7000-37FABE(config-management-policy-default)#telnet
   rfs7000-37FABE(config-management-policy-default)#commit write
   ```

5. Connect to the controller through Telnet using its configured IP address. Use the following credentials when logging on to the device for the first time:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin123</td>
</tr>
</tbody>
</table>

   When logging into the controller for the first time, you are prompted to change the password.

   To change user credentials:

1. Enter the username, password, role and access details.

   ```
   rfs7000-37FABE(config-management-policy-default)#user testuser password test@123
   role helpdesk access all
   rfs7000-37FABE(config-management-policy-default)#commit
   rfs7000-37FABE(config-management-policy-default)#show context
   management-policy default
   telnet
   http server
   https server
   ssh
   user admin password 1
   ba7da2bf2f7945af1d3ae1b8b762b541bd5bac1f80a54c4d4488f38ed44b91ecd role superuser
   access all
   user operator password 1
   0be97e9e30d29d8c4733e7c05f74a7be54570c2450e855cea1a696b0558a40401 role monitor access all
   user testuser password 1
   bca381b5b93cdddb0c209e1da8a9d837fa09bfae14cc987438a4d144cb516ffcb role helpdesk access all
   snmp-server community public ro
   snmp-server community private rw
   snmp-server user snmptrap v3 encrypted des auth md5 0 test@123
   snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
   snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
   rfs7000-37FABE(config-management-policy-default)#
   ```

2. Logon to the Telnet console and provide the user details configured in the previous step to access the controller.

   ```
   rfs7000 release 5.8.1.0-007D
   rfs7000-37FABE login: testuser
   Password:
   Welcome to CLI
   Starting CLI...
   rfs7000-37FABE>
   ```
1.5.3.2 Configuring SSH

*Enabling Remote Administration*

By default, SSH is enabled from the factory settings on the controller. The controller requires an IP address and login credentials.

To enable SSH access in the default profile, login through the serial console. Perform the following:

1. Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

   ```
   rfs7000-37FABE>en
   rfs7000-37FABE#configure
   Enter configuration commands, one per line. End with CNTL/Z.
   ```

2. Go to 'config-management-policy-default' mode.

   ```
   rfs7000-37FABE(config)#management-policy default
   rfs7000-37FABE(config-management-policy-default)#
   ```

3. Enter SSH at the command prompt.

   ```
   rfs7000-37FABE(config-management-policy-default)#ssh
   ```

4. Log into the controller through SSH using appropriate credentials.

5. Use the following credentials when logging on to the device for the first time:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin123</td>
</tr>
</tbody>
</table>

When logging into the controller for the first time, you are prompted to change the password.

To change the user credentials:

```
rfs7000 release 5.8.1.0-007D
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs7000-37FABE>
```
CHAPTER 2
USER EXEC MODE COMMANDS

Logging in to the wireless controller places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before the connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests, and list system information.

To list available USER EXEC commands, use ? at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (>).

<DEVICE>>?
Command commands:
  captive-portal-page-upload  Captive portal advanced page upload
  change-passwd               Change password
  clear                       Clear
  clock                       Configure software system clock
  cluster                     Cluster commands
  commit                      Commit all changes made in this session
  connect                     Open a console connection to a remote device
  create-cluster              Create a cluster
  crypto                      Encryption related commands
  crypto-cmp-cert-update      Update the cmp certs
  database                    Database
  database-backup             Backup database
  database-restore            Restore database
  debug                       Debugging functions
  device-upgrade              Device firmware upgrade
  disable                     Turn off privileged mode command
  enable                      Turn on privileged mode command
  file-sync                   File sync between controller and adoptees
  help                        Description of the interactive help system
  join-cluster                Join the cluster
  l2tpv3                      L2tpv3 protocol
  logging                     Modify message logging facilities
  mint                        MiNT protocol
  no                          Negate a command or set its defaults
  on                          On RF-Domain
  opendns                     Opendns username/password configuration
  page                        Toggle paging
  ping                        Send ICMP echo messages
  ping6                       Send ICMPv6 echo messages
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  smart-cache                 Content Cache Operation
  ssh                         Open an ssh connection
  telnet                      Open a telnet connection
  terminal                   Set terminal line parameters
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time-it</td>
<td>Check how long a particular command took between request and completion of response</td>
</tr>
<tr>
<td>traceroute</td>
<td>Trace route to destination</td>
</tr>
<tr>
<td>traceroute6</td>
<td>Trace route to destination(IPv6)</td>
</tr>
<tr>
<td>virtual-machine</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>watch</td>
<td>Repeat the specific CLI command at a periodic interval</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>exit</td>
<td>Exit from the CLI</td>
</tr>
</tbody>
</table>

*<DEVICE>>*
### 2.1 User Exec Commands

The following table summarizes the User Exec Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal-page-upload</td>
<td>Uploads captive portal advanced pages</td>
<td>page 2-5</td>
</tr>
<tr>
<td>change-passwd</td>
<td>Changes the password of a logged user</td>
<td>page 2-8</td>
</tr>
<tr>
<td>clear</td>
<td>Resets the last saved command</td>
<td>page 2-9</td>
</tr>
<tr>
<td>clock</td>
<td>Configures the system clock</td>
<td>page 2-20</td>
</tr>
<tr>
<td>cluster</td>
<td>Accesses the cluster context</td>
<td>page 2-21</td>
</tr>
<tr>
<td>connect</td>
<td>Establishes a console connection to a remote device</td>
<td>page 2-22</td>
</tr>
<tr>
<td>create-cluster</td>
<td>Creates a new cluster on a specified device</td>
<td>page 2-23</td>
</tr>
<tr>
<td>crypto</td>
<td>Enables encryption</td>
<td>page 2-25</td>
</tr>
<tr>
<td>crypto-cmp-cert-update</td>
<td>Triggers a CMP certificate update on a specified device or devices</td>
<td>page 2-34</td>
</tr>
<tr>
<td>database</td>
<td>Enables automatic repairing (vacuuming) and dropping of databases</td>
<td>page 2-35</td>
</tr>
<tr>
<td>database-backup</td>
<td>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server</td>
<td>page 2-36</td>
</tr>
<tr>
<td>database-restore</td>
<td>Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored to the original database.</td>
<td>page 2-37</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings</td>
<td>page 2-38</td>
</tr>
<tr>
<td>disable</td>
<td>Turns off (disables) the privileged mode command set</td>
<td>page 2-48</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on (enables) the privileged mode command set</td>
<td>page 2-49</td>
</tr>
<tr>
<td>file-sync</td>
<td>Configures parameters enabling syncing of PKCS#12 certificate between the staging-controller and adoptee AP6522/AP6562 client-bridge access points</td>
<td>page 2-50</td>
</tr>
<tr>
<td>join-cluster</td>
<td>Adds a device (access point, wireless controller, or service platform) to an existing cluster of devices</td>
<td>page 2-52</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Establishes or brings down Layer 2 Tunneling Protocol Version 3 (L2TPV3) tunnels</td>
<td>page 2-54</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging facilities</td>
<td>page 2-56</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol</td>
<td>page 2-58</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 2-60</td>
</tr>
<tr>
<td>on</td>
<td>Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, show</td>
<td>page 2-62</td>
</tr>
</tbody>
</table>
### Table 2.1 User Exec Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>opendns</strong></td>
<td>Connects to the OpenDNS site using OpenDNS registered credentials (username, password) to obtain the device-id. This command is a part of the process integrating access points and controllers with the OpenDNS service.</td>
<td>page 2-63</td>
</tr>
<tr>
<td><strong>page</strong></td>
<td>Toggles a device’s (access point, wireless controller, or service platform) paging function</td>
<td>page 2-65</td>
</tr>
<tr>
<td><strong>ping</strong></td>
<td>Sends ICMP echo messages to a user-specified location</td>
<td>page 2-66</td>
</tr>
<tr>
<td><strong>ping6</strong></td>
<td>Sends ICMPv6 echo messages to a user-specified IPv6 address</td>
<td>page 2-68</td>
</tr>
<tr>
<td><strong>ssh</strong></td>
<td>Opens an SSH connection between two network devices</td>
<td>page 2-69</td>
</tr>
<tr>
<td><strong>telnet</strong></td>
<td>Opens a Telnet session</td>
<td>page 2-70</td>
</tr>
<tr>
<td><strong>terminal</strong></td>
<td>Sets the length and width of the terminal window</td>
<td>page 2-71</td>
</tr>
<tr>
<td><strong>time-it</strong></td>
<td>Verifies the time taken by a particular command between request and response</td>
<td>page 2-72</td>
</tr>
<tr>
<td><strong>traceroute</strong></td>
<td>Traces the route to its defined destination</td>
<td>page 2-73</td>
</tr>
<tr>
<td><strong>traceroute6</strong></td>
<td>Traces the route to a specified IPv6 destination</td>
<td>page 2-74</td>
</tr>
<tr>
<td><strong>watch</strong></td>
<td>Repeats a specific CLI command at a periodic interval</td>
<td>page 2-75</td>
</tr>
<tr>
<td><strong>smart-cache</strong></td>
<td>Pre-fetches content cache from the specified list of URLs. This command is specific to the NX45XX, NX65XX, NX9XXX series service platforms.</td>
<td>page 2-77</td>
</tr>
<tr>
<td><strong>virtual-machine</strong></td>
<td>Installs, configures, and monitors the status of virtual machines (VMs). This command is specific to the NX45XX, NX65XX, NX9XXX series service platforms.</td>
<td>page 2-78</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.

**NOTE:** The input parameter <_HOSTNAME>, if used in syntaxes across this chapter, cannot include an underscore (_) character.
2.1.1 captive-portal-page-upload

**User Exec Commands**

Uploads captive portal advanced pages to connected access points. Use this command to provide connected access points with specific captive portal configurations so that they can successfully provision login, welcome, and condition pages to requesting clients attempting to access the wireless network using the captive portal.

---

**NOTE:** Ensure that the captive portal pages uploaded are *.tar files.

---

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

captive-portal-page-upload  [<CAPTIVE-PORTAL-NAME>|cancel-upload|delete-file|load-file]
captive-portal-page-upload  <CAPTIVE-PORTAL-NAME>  [<MAC/HOSTNAME]|all|rf-domain]
captive-portal-page-upload  <CAPTIVE-PORTAL-NAME>  [<MAC/HOSTNAME]|all]
{upload-time  <TIME>}
captive-portal-page-upload  <CAPTIVE-PORTAL-NAME>  rf-domain  [<DOMAIN-NAME]|all]
{from-controller}  {(upload-time  <TIME>))}
captive-portal-page-upload cancel-upload  [<MAC/HOSTNAME]|all|on rf-domain
{[<DOMAIN-NAME]|all]}]
captive-portal-page-upload delete-file  <CAPTIVE-PORTAL-NAME>  <FILE-NAME>
captive-portal-page-upload load-file  <CAPTIVE-PORTAL-NAME>  <URL>

**Parameters**
- captive-portal-page-upload  <CAPTIVE-PORTAL-NAME>  [<MAC/HOSTNAME]|all]
{upload-time  <TIME>)}

<table>
<thead>
<tr>
<th>captive-portal-page-upload  &lt;CAPTIVE-PORTAL-NAME&gt;</th>
<th>Uploads advanced pages of the captive-portal identified by the &lt;CAPTIVE-PORTAL-NAME&gt; parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC/HOSTNAME&gt;</td>
<td>Uploads to a specified AP</td>
</tr>
<tr>
<td>all</td>
<td>Uploads to all APs</td>
</tr>
<tr>
<td>upload-time &lt;TIME&gt;</td>
<td>Optional. Configures an AP upload time</td>
</tr>
</tbody>
</table>

- <CAPTIVE-PORTAL-NAME> — Specify the captive portal’s name (should be existing and configured).
- <MAC/HOSTNAME> — Specify AP’s MAC address or hostname.
- <TIME> — Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.
**captive-portal-page-upload** `<CAPTIVE-PORTAL-NAME>` **rf-domain** `[<DOMAIN-NAME>|all]`

- **from-controller** `{(upload-time <TIME>)}`

  Uploads advanced pages of the captive portal identified by the `<CAPTIVE-PORTAL-NAME>` parameter
  - `<CAPTIVE-PORTAL-NAME>` – Specify captive portal’s name (should be existing and configured).

<table>
<thead>
<tr>
<th>captive-portal-page-upload</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code></td>
</tr>
</tbody>
</table>

- **rf-domain** `[<DOMAIN-NAME>|all]` Uploads to all APs within a specified RF Domain or all RF Domains
  - `<DOMAIN-NAME>` – Uploads to APs within a specified RF Domain. Specify the RF Domain name.
  - `all` – Uploads to APs across all RF Domains

<table>
<thead>
<tr>
<th>rf-domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>`[&lt;DOMAIN-NAME&gt;</td>
</tr>
</tbody>
</table>

- **from-controller** Optional. Uploads to APs from the adopted device

<table>
<thead>
<tr>
<th>from-controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Uploads to APs from the adopted device</td>
</tr>
</tbody>
</table>

- **upload-time** `<TIME>` Optional. Configures an AP upload time
  - `<TIME>` – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.

<table>
<thead>
<tr>
<th>upload-time</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TIME&gt;</code></td>
</tr>
</tbody>
</table>

**captive-portal-page-upload cancel-upload** `[<MAC/ HOSTNAME>|all|on rf-domain `[<DOMAIN-NAME]|all]]`

- Select one of the following options:
  - `<MAC/ HOSTNAME>` – Cancels scheduled upload to a specified AP. Specify the AP’s MAC address or hostname.
  - `all` – Cancels all scheduled AP uploads
  - `on rf-domain` – Cancels all scheduled uploads within a specified RF Domain or all RF Domains
    - `<DOMAIN-NAME>` – Cancels scheduled uploads within a specified RF Domain. Specify RF Domain name.
    - `all` – Cancels scheduled uploads across all RF Domains

<table>
<thead>
<tr>
<th>cancel-upload</th>
</tr>
</thead>
<tbody>
<tr>
<td>`[&lt;MAC/ HOSTNAME&gt;</td>
</tr>
</tbody>
</table>

**captive-portal-page-upload delete-file** `<CAPTIVE-PORTAL-NAME>` `<FILE-NAME>`

- Deletes a captive portal’s, identified by the `<CAPTIVE-PORTAL-NAME>` keyword, uploaded internal page files
  - `<CAPTIVE-PORTAL-NAME>` – Specify the captive portal’s name.
  - `<FILE-NAME>` – Specify the file name. The specified internal captive portal page is deleted.

<table>
<thead>
<tr>
<th>captive-portal-page-upload delete-file</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> <code>&lt;FILE-NAME&gt;</code></td>
</tr>
</tbody>
</table>

**captive-portal-page-upload load-file** `<CAPTIVE-PORTAL-NAME>` `<URL>`

- Loads captive-portal advanced pages
  - Specify the captive portal’s name and location. The captive portal should be existing and configured.
  - `<URL>` – Specifies location of the captive-portal’s advanced pages. Use one of the following formats to specify the location:

<table>
<thead>
<tr>
<th>captive-portal-page-upload load-file</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> <code>&lt;URL&gt;</code></td>
</tr>
</tbody>
</table>
IPv4 URLs:
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
  - sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
  - http://<hostname|IP>[:port]/path/file
  - cf:/path/file
  - usb<n>:/path/file

IPv6 URLs:
  - tftp://<hostname>[IPv6]>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname>[IPv6]>[:port]/path/file
  - sftp://<user>:<passwd>@<hostname>[IPv6]>[:port]/path/file

**Note:** The captive portal pages are downloaded to the controller from the location specified here. After downloading use the `captive-portal-page-upload > <CAPTIVE-PORTAL-NAME> > <DEVICE-OR-DOMAIN-NAME>` command to upload these pages to APs.

**Examples**

```
ap6562-B1A214>captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/pages_new_only.tar
```

```
ap6562-B1A214>show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
```

```
ap6562-B1A214>captive-portal-page-upload captive_portal_test all
-----------------------------------------------------------------------
CONTROLLER         STATUS                  MESSAGE
-----------------------------------------------------------------------
FC-0A-81-B1-A2-14   Success                Added 6 APs to upload queue
-----------------------------------------------------------------------
```

```
ap6562-B1A214>show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0
-----------------------------------------------------------------------
AP          STATE          UPLOAD TIME  PROGRESS  RETRIES  LAST UPLOAD ERROR  UPLOADED BY
-----------------------------------------------------------------------
ap6562-B1A738 downloading  immediate    100   0        -                  None
-----------------------------------------------------------------------
```

```
ap6562-B1A214>
```
2.1.2 change-passwd

User Exec Commands

Changes the password of a logged user. When this command is executed without any parameters, the password can be changed interactively.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
change-passwd \{<OLD-PASSWORD>\} <NEW-PASSWORD>

Parameters
- change-passwd \{<OLD-PASSWORD>\} <NEW-PASSWORD>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;OLD-PASSWORD&gt;</td>
<td>Optional. Specify the password to be changed.</td>
</tr>
<tr>
<td>&lt;NEW-PASSWORD&gt;</td>
<td>Specify the new password.</td>
</tr>
</tbody>
</table>

Note: The password can also be changed interactively. To do so, press [Enter] after the command.

Usage Guidelines

A password must be from 1 - 64 characters.

Examples
rfs7000-37FABE>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory\{write memory\} to be persistent.
rfs7000-37FABE#write memory
OK
rfs7000-37FABE>
2.1.3 clear

**User Exec Commands**

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared, using this command, depends on the mode where the clear command is executed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

clear [arp-cache|bonjour|cdp|counters|crypto|event-history|gre|ip|ipv6|lldp|mac-address-table|mint|role|rtls|smart-cache|spanning-tree|traffic-shape|vrrp]
clear arp-cache {on <DEVICE-NAME>}
clear bonjour cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear counters [ap|radio|wireless-client]
clear counters [ap {<MAC>}|radio {<MAC>/DEVICE-NAME>} {<1-X>]|wireless-client {<MAC>}]
{on <DEVICE-OR-DOMAIN-NAME>}
clear crypto [ike|ipsec] sa
clear crypto ike sa [{<IP>}|all] {on <DEVICE-NAME>}
clear crypto ipsec sa {on <DEVICE-NAME>}
clear event-history
clear gre stats {on <DEVICE-NAME>}
clear ip [bgp|dhcp|ospf]
clear ip bgp [{<IP>}|all external|process]
clear ip bgp [{<IP>}|all external] {in|on|out|soft}
clear ip bgp [{<IP>}|all external] {in prefix-filter} {on <DEVICE-NAME>}
clear ip bgp [{<IP>}|all external] {out} {on <DEVICE-NAME>}
clear ip bgp [{<IP>}|all external] {soft {in|out}} {on <DEVICE-NAME>}
clear ip bgp process {on <DEVICE-NAME>}
clear ip dhcp bindings [{<IP>}|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}
clear ipv6 neighbor-cache {on <DEVICE-NAME>}
clear mac-address-table {address|interface|vlan} {on <DEVICE-NAME>}
clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table {interface [<IF-NAME>|ge <1-X]|port-channel <1-X>|t1e1 <1-4>|<1-1>|up <1-X>|vmif <1-X>|xge <1-4>} {on <DEVICE-NAME>}
clear mint mlcp history {on <DEVICE-NAME>}
clear role ldap-stats {on <DEVICE-NAME>}

**NOTE:** When using the `clear` command, refer to the interface details provided in Chapter 7, `interface`.
clear rtls [aeroscout|ekahau] 
{<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}}

clear spanning-tree detected-protocols {interface|on} 
{on <DEVICE-NAME>}

clear spanning-tree detected-protocols {interface [{INTERFACE-NAME}|ge <1-X>|me1|port-channel <1-X>|pppoe1|up|vian <1-4094>|wwan1|vmif <1-X}> {on <DEVICE-NAME>}

clear traffic-shape statistics class <1-4> {on <DEVICE-NAME>}

clear vrrp [error-stats|stats] {on <DEVICE-NAME>}

The following clear command is specific to the NX45XX, NX65XX, and NX9XXX series service platforms:
clear smart-cache storage [all|url-regex <WORD>] {on <DEVICE-NAME>}

Parameters

<table>
<thead>
<tr>
<th>clear arp-cache {on &lt;DEVICE-NAME&gt;}</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp-cache</td>
</tr>
<tr>
<td>Clears Address Resolution Protocol (ARP) cache entries on a device. This protocol matches layer 3 IP addresses to layer 2 MAC addresses.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; Optional. Clears ARP cache entries on a specified device</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear bonjour cache {on &lt;DEVICE-NAME&gt;}</th>
</tr>
</thead>
<tbody>
<tr>
<td>bonjour cache</td>
</tr>
<tr>
<td>Clears all Bonjour cached statistics. Once cleared the system has to re-discover available Bonjour services.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; Optional. Clears all Bonjour cached statistics on a specified device</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

| clear [cdp|lldp] neighbors {on <DEVICE-NAME>} |
|-----------------------------------------------|
| cdp                                            |
| Clears Cisco Discovery Protocol (CDP) table entries |
| lldp                                           |
| Clears Link Layer Discovery Protocol (LLDP) table entries |
| neighbors                                      |
| Clears CDP or LLDP neighbor table entries based on the option selected in the preceding step |
| on <DEVICE-NAME> Optional. Clears CDP or LLDP neighbor table entries on a specified device |
| • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

| clear counters [ap {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-X>}|wireless-client {<MAC>}] {on <DEVICE-OR-DOMAIN-NAME>} |
|--------------------------------------------------------|
| counters                                               |
| Clears counters based on the parameters passed. The options are: AP, radio, and wireless clients. |
| ap <MAC>                                               |
| Clears counters for all APs or a specified AP         |
| • <MAC> – Optional. Specify the AP’s MAC address.     |

Note: If no MAC address is specified, all AP counters are cleared.
### USER EXEC MODE COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear crypto ike sa</code> [IP]</td>
<td>Clears encryption module database for IKE security associations (SAs) for the peer identified by the IP keyword.</td>
</tr>
<tr>
<td><code>&lt;MAC/DEVICE-NAME&gt;</code></td>
<td>Clears radio interface counters on a specified device or on all devices.</td>
</tr>
<tr>
<td><code>&lt;1-X&gt;</code></td>
<td>Specifies the radio interface by its index.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Clears IKE SA entries on a specified device.</td>
</tr>
<tr>
<td><code>clear crypto ipsec sa</code> [IP]</td>
<td>Clears encryption module database for IPSec SAs.</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>Clears counters for all wireless clients or a specified wireless client.</td>
</tr>
<tr>
<td><code>wireless-client</code></td>
<td>Specifies the wireless client's MAC address.</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>Clears GRE tunnel statistics on a specified device.</td>
</tr>
<tr>
<td><code>gre stats</code></td>
<td>ClearsGRE tunnel statistics.</td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code></td>
<td>Clears event history cache entries.</td>
</tr>
<tr>
<td><code>event-history</code></td>
<td>Specifies the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Note:** If no device name or MAC address is specified, all radio interface counters are cleared.

**Example:**
```
clear crypto ike sa [IP] all {on <DEVICE-NAME>}
```

**Note:** If no MAC address is specified, all wireless client counters are cleared.

**Example:**
```
clear crypto ipsec sa {on <DEVICE-NAME>}
```

**Note:** If no MAC address is specified, all GRE tunnel statistics are cleared.

**Example:**
```
clear gre stats {on <DEVICE-NAME>}
```

**Note:** If no device name is specified, all event history cache entries are cleared.

**Example:**
```
clear event-history
```
- clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}

```
ip bgp [<IP>|all|external] Clears on-going BGP sessions based on the option selected
  • <IP> – Clears BGP session with the peer identified by the <IP> keyword. Specify the BGP peer’s IP address.
  • all – Clears all BGP peer sessions
  • external – Clears external BGP (eBGP) peer sessions
This command is applicable only to the RFS4000, RFS6000, NX45XX, NX65XX, NX9000, NX9600 platforms.
Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy etc.) take effect only after on-going BGP sessions are cleared.
The clear > ip > bgp command clears BGP sessions. To reduce lose of route updates during the process, use the ‘soft’ option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage.
in prefix-filter Optional. Clears inbound route updates
  • prefix-filter – Optional. Clears the existing Outbound Route Filtering (ORF) prefix-list
on <DEVICE-NAME> Optional. Clears route updates on a specified device
  • <DEVICE-NAME> – Specify the name of the AP or service platform.
```

- clear ip bgp [<IP>|all|external] {out} {on <DEVICE-NAME>}

```
out Optional. Clears outbound route updates. Optionally specify the device on which to execute this command.
on <DEVICE-NAME> The following keyword is recursive and optional.
  • on <DEVICE-NAME> – Optional. Clears BGP sessions on a specified device
  • <DEVICE-NAME> – Specify the name of the AP or service platform.
```

- clear ip bgp [<IP>|all|external] {soft {in|out}} {on <DEVICE-NAME>}

```
ip bgp [ <IP>|all|external] Clears on-going BGP sessions based on the option selected
  • <IP> – Clears the BGP peer session with the peer identified by the <IP> keyword. Specify the BGP peer’s IP address.
  • all – Clears all BGP peer sessions
  • Contd..
<table>
<thead>
<tr>
<th>USER EXEC MODE COMMANDS 2-13</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear ip bgp process</strong> {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td><strong>ip bgp process</strong> clears all BGP processes running. This command is applicable only to the RFS4000, RFS6000, NX45XX, NX65XX, NX9000, and NX9600 platforms.</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong> Optional. Clears all BGP processes on a specified device</td>
</tr>
<tr>
<td><strong>&lt;DEVICE-NAME&gt;</strong> – Specify the name of the AP or service platform.</td>
</tr>
<tr>
<td><strong>clear ip dhcp bindings</strong> [&lt;IP&gt;</td>
</tr>
<tr>
<td><strong>ip dhcp bindings</strong> clears DHCP connections and server bindings.</td>
</tr>
<tr>
<td><strong>&lt;IP&gt;</strong> clears specific address binding entries. Specify the IP address to clear binding entries.</td>
</tr>
<tr>
<td><strong>all</strong> clears all address binding entries.</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong> Optional. Clears a specified address binding or all address bindings on a specified device</td>
</tr>
<tr>
<td><strong>&lt;DEVICE-NAME&gt;</strong> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><strong>clear ip ospf process</strong> {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td><strong>ip ospf process</strong> clears already enabled Open Shortest Path First (OSPF) process and restarts the process.</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong> Optional. Clears OSPF process on a specified device</td>
</tr>
<tr>
<td>OSPF is a link-state interior gateway protocol (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighboring routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets.</td>
</tr>
<tr>
<td><strong>&lt;DEVICE-NAME&gt;</strong> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>
- **clear ipv6 neighbor-cache {on <DEVICE-NAME>}**
  
  clears IPv6 neighbor cache entries

- **clear ipv6 neighbor-cache {on <DEVICE-NAME>}**
  
  Optional. Clears IPv6 neighbor cache entries on a specified device
  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

- **clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}**
  
  clears the MAC address forwarding table

  • address <MAC> Optional. Clears a specified MAC address from the MAC address table.
    
    • <MAC> – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF

  • vlan <1-4094> Optional. Clears all MAC addresses for a specified VLAN
    
    • <1-4094> – Specify the VLAN ID from 1 - 4094.

  • on <DEVICE-NAME> Optional. Clears a single MAC entry or all MAC entries, for the specified VLAN on a specified device
    
    • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

    On the NX45XX and NX65XX series service platform, this command clears the MAC address forwarding table on the device's hardware and not the dataplane.

- **clear mac-address-table interface [{<IF-NAME>|ge <1-X>|port-channel <1-X>|t1e1 <1-4> <1-1>|up <1-2>|vmif <1-X>|xge <1-4>} {on <DEVICE-NAME>}**
  
  clears the MAC address forwarding table

  • interface Clears all MAC addresses for the selected interface. Use the options available to specify the interface.

  • <IF-NAME> Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port)
    
    • <IF-NAME> – Specify the layer 2 interface name.

  • ge <1-X> Clears MAC address forwarding table for the specified GigabitEthernet interface
    
    • <1-X> – Specify the GigabitEthernet interface index from 1 - X.
    
    The number of Ethernet interfaces supported varies for different device types. For example, the NX45XX and NX65XX support 24 GE interfaces. Where as, RFS4000 supports 5 GE interfaces.

  • port-channel <1-X> Clears MAC address forwarding table for the specified port-channel interface
    
    • <1-X> – Specify the port-channel interface index from 1 - X.
    
    The number of port-channel interfaces supported varies for different device types. For example, the NX45XX and NX65XX support 13 port-channels. Where as, RFS4000 supports 3 port-channels.

  • t1e1 <1-4> <1-1> Clears MAC address forwarding table for the specified T1E1L interface
    
    • <1-4> – Specify the T1E1 interface index from 1 - 4. A maximum of 4 slots are available. Select the slot to clear the MAC address forwarding table.
    
    • <1-1> – Specify the T1E1 port ID from 1 - 1.
    
    The T1E1 interfaces are supported only on the NX45XX and NX65XX series service platforms.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **up <1-X>**  | Clears MAC address forwarding table for the WAN Ethernet interface  
The number of WAN Ethernet interfaces supported varies for different devices. The RFS4000 and RFS6000 devices support 1 WAN Ethernet interface. The NX45XX supports 2 WAN Ethernet interfaces. |
| **vmif <1-X>**| Clears MAC address forwarding table for the VM interface  
• `<1-X>` – Specify the VM interface index from 1 - X.  
The VMIF interfaces are supported only on the NX45XX, NX65XX, NX9500, and NX9510 series service platforms. The number of supported VMIFs varies for different device types. |
| **xge <1-4>` | Clears MAC address forwarding table for the specified TenGigabitEthernet interface  
• `<1-4>` – Specify the GigabitEthernet interface index from 1 - 4.  
This interface is supported only on the NX9000 series service platforms. |
| **on <DEVICE-NAME>** | Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device  
• `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |

- clear mint mlcp history `{on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mint</strong></td>
<td>Clears MiNT related information</td>
</tr>
<tr>
<td><strong>mlcp history</strong></td>
<td>Clears <em>MiNT Link Creation Protocol</em> (MLCP) client history</td>
</tr>
</tbody>
</table>
| **on <DEVICE-NAME>** | Optional. Clears MLCP client history on a specified device  
• `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |

- clear role ldap-stats `{on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>role ldap-stats</strong></td>
<td>Clears <em>Lightweight Directory Access Protocol</em> (LDAP) server statistics</td>
</tr>
</tbody>
</table>
| **on <DEVICE-NAME>** | Optional. Clears LDAP server statistics on a specified device  
• `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |

- clear rtls [aeroscout|ekahau] `{<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>rtls</strong></td>
<td>Clears <em>Real Time Location Service</em> (RTLS) statistics</td>
</tr>
<tr>
<td><strong>aeroscout</strong></td>
<td>Clears RTLS Aeroscout statistics</td>
</tr>
<tr>
<td><strong>ekahau</strong></td>
<td>Clears RTLS Ekahau statistics</td>
</tr>
</tbody>
</table>
| `<MAC/DEVICE-NAME>` | This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.  
• `<MAC/DEVICE-NAME>` – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, or service platform. Specify the AP’s MAC address or hostname. |
| **on <DEVICE-OR-DOMAIN-NAME>** | This keyword is common to the ‘aeroscout’, ‘ekahau’, and <MAC/DEVICE-NAME> parameters.  
| on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified device  
| <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain  |

| **clear spanning-tree detected-protocols {on <DEVICE-NAME>}** |

| **spanning-tree** | Clears spanning tree entries on an interface, and restarts protocol migration  |
| **detected-protocols** | Restarts protocol migration  |
| **on <DEVICE-NAME>** | Optional. Clears spanning tree entries on a specified device  
| <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.  |

| **clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-X>|me1|port-channel <1-X>|pppoe1|up1|vlan <1-4094>|wwan1|vmif <1-X>]} {on <DEVICE-NAME>}** |

| **spanning-tree** | Clears spanning tree entries on an interface and restarts protocol migration  |
| **detected-protocols** | Restarts protocol migration  |
| **interface** | Optional. Clears spanning tree entries on different interfaces  
| [<INTERFACE-NAME>]  
| ge <1-X>|me1|port-channel <1-X>|pppoe1|up1|vlan <1-4094>|wwan1|vmif <1-X>]  
| **on <DEVICE-NAME>** | Optional. Clears spanning tree entries on a specified device  
| <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.  |

**spanning-tree** Clears spanning tree entries on an interface, and restarts protocol migration  
**detected-protocols** Restarts protocol migration  
**interface** Optional. Clears spanning tree entries on different interfaces  
<INTERFACE-NAME> – Clears detected spanning tree entries on a specified interface. Specify the interface name.  
ge <1-X> – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - X.  
The number of Ethernet interfaces supported varies for different device types. For example the NX45XX and NX65XX support 24 GE interfaces. Where as, RFS4000 supports 5 GE interfaces.  
me1 – Clears FastEthernet interface spanning tree entries  
port-channel <1-X> – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - X.  
The number of port-channel interfaces supported varies for different device types. For example the NX45XX and NX65XX support 13 port-channels. Where as, RFS4000 supports 3 port-channels.  
pppoe1 – Clears detected spanning tree entries for Point-to-Point Protocol over Ethernet (PPPoE) interface  
up1 – Clears detected spanning tree entries for the WAN Ethernet interface  
vlan <1-4094> – Clears detected spanning tree entries for the selected VLAN interface. Select a Switch Virtual Interface (SVI) VLAN ID from 1- 4094.  
wwan1 – Clears detected spanning tree entries for wireless WAN interface.  
vmif <1-X> – Clears detected spanning tree entries for VM interfaces  
The VMIF interfaces are supported only on the NX45XX, NX65XX, NX9500, and NX9510 series service platforms. The number of supported VMIFs varies for different device types.  
on <DEVICE-NAME> Optional. Clears spanning tree entries on a specified device  
<DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
### clear traffic-shape statistics class <1-4> {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>traffic-shape statistics</th>
<th>Clears traffic shaping statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>class &lt;1-4&gt;</td>
<td>Clears traffic shaping statistics for a specific traffic class</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4&gt; – Specify the traffic class from 1 - 4.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the traffic class is not specified, the system clears all traffic shaping statistics.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears traffic shaping statistics for the specified traffic class on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the access point, wireless controller, or service platform.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For more information on configuring traffic-shape, see traffic-shape.</td>
</tr>
</tbody>
</table>

### clear vrrp [error-stats|stats] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>vrrp</th>
<th>Clears a device’s Virtual Router Redundancy Protocol (VRRP) statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.</td>
</tr>
<tr>
<td>error-stats</td>
<td>Clears global error statistics</td>
</tr>
<tr>
<td>stats</td>
<td>Clears VRRP related statistics</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to the ‘error-stats’ and ‘stats’ parameters:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Clears VRRP statistics on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

### clear smart-cache storage [all|url-regex <WORD>] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>smart-cache</th>
<th>Clears the smart-cache storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Smart caching is a licensed service available on the NX45XX and NX65XX series service platforms. It allows the temporary storage of frequently accessed Web content (Web pages, graphics, audio and video files etc.) on network infrastructure devices. When this content is requested, it is retrieved from a local content cache and not from the origin server. For more information on enabling content caching, see smart-cache-policy.</td>
</tr>
<tr>
<td>storage [all</td>
<td>regex &lt;WORD&gt;]</td>
</tr>
<tr>
<td></td>
<td>• all – Clears all cached content</td>
</tr>
<tr>
<td></td>
<td>• regex &lt;WORD&gt; – Clears only those URLs matching the specified expression</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Provide the URL in the following format: e.g. \xxx|+.(flv</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears stored content on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>
Examples

rfs4000-229D58>clear event-history

rfs4000-229D58>clear spanning-tree detected-protocols interface port-channel 1

rfs4000-229D58>clear spanning-tree detected-protocols interface ge 1

rfs4000-229D58>show lldp neighbors
-------------------------
Chassis ID: 00-23-68-88-0D-A7
System Name: rfs4000-880DA7
Platform: RFS-4011-11110-US, Version 5.8.1.0-022D
Capabilities: Bridge WLAN Access Point Router
Enabled Capabilities: Bridge WLAN Access Point Router
Local Interface: ge5, Port ID (outgoing port): ge5
TTL: 176 sec
Management Addresses: 192.168.13.8,192.168.0.1,1.2.3.4
rfs4000-229D58>
rfs4000-229D58>clear lldp neighbors

rfs4000-229D58>show lldp neighbors

rfs4000-229D58>show cdp neighbors
--------------------------------------------------------------------------------
Device ID           Platform        Local Intrfce    Port ID      Duplex
--------------------------------------------------------------------------------
  rfs4000-880DA7    RFS-4011-11110-US    ge1              ge1        full
  rfs7000-37FDF2    RFS-7010-1000-WR     ge1              ge1        full
  rfs6000-434CAA    RFS6000              ge1              ge1        full
  ap7131-139B34    AP7131N              ge1              ge1        full
--------------------------------------------------------------------------------
rfs4000-229D58>
rfs4000-229D58>clear cdp neighbors

rfs4000-229D58>show cdp neighbors
--------------------------------------------------------------------------------
Device ID         Platform     Local Intrfce      Port ID        Duplex
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
rfs4000-229D58>
rfs4000-229D58>clear role ldap-stats

rfs4000-229D58>show role ldap-stats
No ROLE LDAP statistics found.
rfs4000-229D58>
rfs4000-229D58>show mac-address-table

<table>
<thead>
<tr>
<th>BRIDGE</th>
<th>VLAN</th>
<th>PORT</th>
<th>MAC</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-02-B3-28-D1-55</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-0F-8F-19-BA-4C</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-5C-FA-8E</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-23-68-0F-43-D8</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-15-70-38-06-49</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-23-68-13-9B-34</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-58-72-58</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-15-70-81-74-2D</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-5C-FA-2B</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-15-70-37-FD-F2</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-6C-88-09</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-71-17-28</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>5C-0E-8B-18-10-91</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>3C-CE-73-F4-47-83</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-23-68-88-0D-AC</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-A0-F8-68-D5-5C</td>
<td>forward</td>
</tr>
</tbody>
</table>

Total number of MACs displayed: **16**

rfs4000-229D58>

rfs4000-229D58>clear mac-address-table address 00-02-B3-28-D1-55

In the following example the first MAC address in the table has been cleared. Now the table has only 15 entries.

rfs4000-229D58>show mac-address-table

<table>
<thead>
<tr>
<th>BRIDGE</th>
<th>VLAN</th>
<th>PORT</th>
<th>MAC</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-0F-8F-19-BA-4C</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-5C-FA-8E</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-23-68-0F-43-D8</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-15-70-38-06-49</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-23-68-13-9B-34</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-58-72-58</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-15-70-81-74-2D</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-5C-FA-2B</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-15-70-37-FD-F2</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-6C-88-09</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>B4-C7-99-71-17-28</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>5C-0E-8B-18-10-91</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>3C-CE-73-F4-47-83</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-23-68-88-0D-AC</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>ge5</td>
<td>00-A0-F8-68-D5-5C</td>
<td>forward</td>
</tr>
</tbody>
</table>

Total number of MACs displayed: **15**

rfs4000-229D58>
2.1.4 clock

User Exec Commands

Sets a device’s system clock. By default all WiNG devices are shipped with the time zone and time format set to UTC and 24-hour clock respectively. If a device’s clock is set without resetting the time zone, the time is displayed relative to the *Universal Time Coordinated* (UTC) – Greenwich Time. For example, San Jose is approximately 7 or 8 hours (depending on the time of the year) behind the UTC time. If the time at Greenwich, UK is 15:00:00 UTC, at San Jose it will display as 8:00:00 or 7:00:00 UTC. To display time in the local time zone format, in the device’s configuration mode, use the timezone command to reset the time zone. You can also reset the time zone at the RF Domain level. When configured as RF Domain setting, it applies to all devices within the domain. Configuring the local time zone prior to setting the clock is recommended. For more information on configuring RF Domain time zone, see `timezone`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}

Parameters

- `<HH:MM:SS>` Sets the current time (in military format hours, minutes, and seconds)
  
  *Note:* By default, the WiNG software displays time in the 24-hour clock format. This setting cannot be changed.

- `<1-31>` Sets the numerical day of the month

- `<MONTH>` Sets the month of the year (Jan to Dec)

- `<1993-2035>` Sets a valid four digit year from 1993 - 2035

- `on <DEVICE-NAME>` Optional. Sets the clock on a specified device
  
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

Examples

The following commands set the time zone and clock for the logged device:

```
nx4500-5CFA8E(config-device-B4-C7-99-5C-FA-8E)#timezone America/Los_Angeles
```

```
nx4500-5CFA8E>clock set 10:13:00 24 Mar 2015
```

```
nx4500-5CFA8E>show clock
2015-03-24 10:13:07 PDT
```

Note, if the clock is set without resetting the time zone, the time displays as UTC time, as shown in the following example:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show clock
2015-09-07 08:55:23 UTC
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```
2.1.5 cluster

User Exec Commands

Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.

Commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

cluster start-election

Parameters

- cluster start-election

| start-election | Starts a new cluster master election |

Examples

rfs7000-37FABE>cluster start-election
rfs7000-37FABE>

Related Commands

<table>
<thead>
<tr>
<th>create-cluster</th>
<th>Creates a new cluster on the specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td>join-cluster</td>
<td>Adds a wireless controller or service platform, as a member, to an existing cluster of controllers</td>
</tr>
</tbody>
</table>
2.1.6 connect

User Exec Commands

Begins a console connection to a remote device using the remote device’s MiNT ID or name

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]

Parameters

- connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]

<table>
<thead>
<tr>
<th>mint-id &lt;MINT-ID&gt;</th>
<th>Connects to the remote system using its MiNT ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;MINT-ID&gt; – Specify the remote device’s MiNT ID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;REMOTE-DEVICE-NAME&gt;</th>
<th>Connects to the remote system using its name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;REMOTE-DEVICE-NAME&gt; – Specify the remote device’s name.</td>
</tr>
</tbody>
</table>

Examples

nx4500-5CFA2B>show mint lsp-db
6 LSPs in LSP-db of 19.5C.FA.2B:
LSP 19.58.72.58 at level 1, hostname "ap5142-587258", 5 adjacencies, seqnum 643541
LSP 19.5C.FA.2B at level 1, hostname "nx4500-5CFA2B", 5 adjacencies, seqnum 293584
LSP 19.5C.FA.8E at level 1, hostname "nx4500-5CFA8E", 5 adjacencies, seqnum 291299
LSP 19.6C.88.09 at level 1, hostname "nx9500-6C8809", 5 adjacencies, seqnum 292181
LSP 19.6D.CD.4B at level 1, hostname "rfs7000-6DCD4B", 5 adjacencies, seqnum 129177
LSP 19.71.17.28 at level 1, hostname "ap8132-711728", 5 adjacencies, seqnum 323509
nx4500-5CFA2B>

nx4500-5CFA2B>connect mint-id 19.71.17.28

Entering character mode
Escape character is '^]'.

AP8132 release 5.8.1.0-020
Dap8132-711728 login:
### 2.1.7 create-cluster

*User Exec Commands*

Creates a new device cluster with the specified name and assigns it an IP address and routing level.

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

**Parameters**

- `create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}`

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
</table>
| name      | Configures the cluster name
| <CLUSTER-NAME> | - Specify a cluster name. Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters. |
| ip         | Specifies the device's IP address used for cluster creation
| <IP>      | - Specify the device's IP address in the A.B.C.D format. |
| level [1|2]  | Optional. Configures the cluster’s routing level
| 1         | - Configures level 1 (local) routing |
| 2         | - Configures level 2 (inter-site) routing |

**Examples**

```plaintext
rfs4000-229D58>create-cluster name TechPubs ip 192.168.13.13 level 1
... creating cluster
... committing the changes
... saving the changes
Please Wait.
[OK]
```

```plaintext
rfs4000-229D58>
```

```plaintext
rfs4000-229D58>show context
```

```plaintext
! Configuration of RFS4000 version 5.8.1.0-020D
!
!
version 2.3
!
!
client-identity Android-2-2
dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
ipv6 enable
no ipv6 request-dhcpv6-options
ipv6 address 2001:10:10:10:10:10:10:2/64
interface vlan2
```
ip address 1.2.3.5/24
no ipv6 enable
no ipv6 request-dhcpv6-options
cluster name TechPubs
cluster mode active
cluster member ip 192.168.13.13 level 1
cluster member ip 192.168.13.8 level 1
logging on
logging console debugging
logging buffered warnings
!
end
rfs4000-229D58>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.</td>
</tr>
<tr>
<td>join-cluster</td>
<td>Adds a device, as a member, to an existing cluster of devices</td>
</tr>
</tbody>
</table>
2.1.8 crypto

User Exec Commands

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by CAs and contain user or device specific information, such as name, public key, IP address, serial number, company name etc. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate Certificate Signing Request (CSR).

This command also enables trustpoint configuration. Trustpoints contain the CA's identity and configuration parameters.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

crypto [key|pki]
crypto key [export|generate|import|zeroize]
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background|on|passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
crypto pki [authenticate|export|generate|import|zeroize]
crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL> {background}
{(on <DEVICE-NAME>)}
crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME>
{autogen-subject-name|subject-name}
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name <EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>, ip-address <IP>
crypto pki export request [generate-rsa-key|short |generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
<ORGANIZATION> <ORGANIZATION-UNIT> <EXPORT-TO-URL>,email <SEND-TO-EMAIL>, fqdn <FQDN>,ip-address <IP>
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL>
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> autogen-subject-name <EMAIL >>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY>
<ORI7ANIZATION> <ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>, ip-address <IP>,on <DEVICE-NAME>)}
crypto pki import [certificate|crl|trustpoint]
    crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
        {background} {(on <DEVICE-NAME>)}
    crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
        {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
    crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}

**Parameters**

- **crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>**
  {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export rsa</td>
<td>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</td>
</tr>
<tr>
<td>&lt;RSA-KEYPAIR-NAME&gt;</td>
<td>Exports an existing RSA Keypair to a specified destination</td>
</tr>
<tr>
<td>&lt;EXPORT-TO-URL&gt;</td>
<td>Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported. After specifying the destination address (where the RSA Keypair is exported), configure one of the following parameters: background or passphrase.</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on.</td>
</tr>
<tr>
<td>passphrase</td>
<td>Optional. Encrypts RSA Keypair before exporting</td>
</tr>
<tr>
<td>&lt;KEY-PASSPHRASE&gt;</td>
<td>• &lt;KEY-PASSPHRASE&gt; – Specify a passphrase to encrypt the RSA Keypair.</td>
</tr>
<tr>
<td>background</td>
<td>• background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following parameter is recursive and common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Performs export operation on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- **crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] **
  {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generate rsa</td>
<td>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</td>
</tr>
<tr>
<td>&lt;RSA-KEYPAIR-NAME&gt; [2048</td>
<td>4096]</td>
</tr>
<tr>
<td></td>
<td>• &lt;RSA-KEYPAIR-NAME&gt; – Specify the RSA Keypair name.</td>
</tr>
<tr>
<td></td>
<td>• [2048</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Generates the new RSA Keypair on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- **crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>**
  {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **import rsa** <RSA-KEYPAIR-NAME> | Imports a RSA Keypair from a specified source  
  - `<RSA-KEYPAIR-NAME>` – Specify the RSA Keypair name. |
| `<IMPORT-FROM-URL>` | Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported.  
  After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase. |
| **background** | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| **passphrase** <KEY-PASSPHRASE> background | Optional. Decrypts the RSA Keypair after importing  
  - `<KEY-PASSPHRASE>` – Specify the passphrase to decrypt the RSA Keypair.  
  - **background** – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point, controller, or service platform) to perform the import on. |
| **on <DEVICE-NAME>** | The following parameter is recursive and common to the ‘background’ and ‘passphrase’ keywords:  
  - **on <DEVICE-NAME>** – Optional. Performs import operation on a specific device  
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |
| **crypto key zeroize rsa** <RSA-KEYPAIR-NAME> `{force} {on <DEVICE-NAME>}` | Deletes a specified RSA Keypair  
  - `<RSA-KEYPAIR-NAME>` – Specify the RSA Keypair name.  
  **Note:** All device certificates associated with this key will also be deleted. |
| **force** | Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion. |
| **on <DEVICE-NAME>** | The following parameter is recursive and optional:  
  - **on <DEVICE-NAME>** – Optional. Deletes all certificates associated with the RSA Keypair on a specified device  
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |
| **crypto pki authenticate** <TRUSTPOINT-NAME> <URL> `{background} {on <DEVICE-NAME>}` | Enables Private Key Infrastructure (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated Certificate Authority (CA) certificates.  
  - **authenticate** <TRUSTPOINT-NAME> | Authenticates a trustpoint and imports the corresponding CA certificate  
    - `<TRUSTPOINT-NAME>` – Specify the trustpoint name.  
  - `<URL>` | Specify CA's location. Both IPv4 and IPv6 address formats are supported.  
    - **Note:** The CA certificate is imported from the specified location. |
| **background** | Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point, controller, or service platform) to perform the export on. |
| **on <DEVICE-NAME>** | The following parameter is recursive and optional:  
  - on <DEVICE-NAME> – Optional. Performs authentication on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>**  
**autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)**  
**pki** Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.  
**export request** Exports CSR to the CA for digital identity certificate. The CSR contains applicant’s details and RSA Keypair’s public key.  
**[generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>** Generates a new RSA Keypair or uses an existing RSA Keypair  
  - generate-rsa-key – Generates a new RSA Keypair for digital authentication  
  - use-rsa-key – Uses an existing RSA Keypair for digital authentication  
  - <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.  
**autogen-subject-name** Auto generates subject name from configuration parameters. The subject name identifies the certificate.  
**<EXPORT-TO-URL>** Specify the CA’s location. Both IPv4 and IPv6 address formats are supported.  
**email <SEND-TO-EMAIL>** Exports CSR to a specified e-mail address  
**fqdn <FQDN>** Exports CSR to a specified Fully Qualified Domain Name (FQDN)  
**ip-address <IP>** Exports CSR to a specified device or system  

**crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)**  
**pki** Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.  
**export request** Exports CSR to the CA for a digital identity certificate. The CSR contains applicant’s details and RSA Keypair’s public key.  
**[generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-key] <RSA-KEYPAIR-NAME>** Generates a new RSA Keypair or uses an existing RSA Keypair  
  - generate-rsa-key – Generates a new RSA Keypair for digital authentication  
  - short [generate-rsa-key|use-rsa-key] – Generates and exports a shorter version of the CSR  
  - use-rsa-key – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it.  
Contd..
- **use-rsa-key** – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name.
- **use-rsa-key** – Uses an existing RSA Keypair for digital authentication
  - `<RSA-KEYPAIR-NAME>` – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.

**subject-name**

| `<COMMON-NAME>` | Configures a subject name, defined by the `<COMMON-NAME>` keyword, to identify the certificate
| | • `<COMMON-NAME>` – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).

**<COUNTRY>**

Sets the deployment country code (2 character ISO code)

**<STATE>**

Sets the state name (2 to 64 characters in length)

**<CITY>**

Sets the city name (2 to 64 characters in length)

**<ORGANIZATION>**

Sets the organization name (2 to 64 characters in length)

**<ORGANIZATION-UNIT>**

Sets the organization unit (2 to 64 characters in length)

**<EXPORT-TO-URL>**

Specify the CA's location. Both IPv4 and IPv6 address formats are supported.
- The CSR is exported to the specified location.

**email**

| `<SEND-TO-EMAIL>` | Exports CSR to a specified e-mail address
| | • `<SEND-TO-EMAIL>` – Specify the CA's e-mail address.

**fqdn <FQDN>**

Exports CSR to a specified FQDN
- `<FQDN>` – Specify the CA's FQDN.

**ip-address <IP>**

Exports CSR to a specified device or system
- `<IP>` – Specify the CA's IP address.

- **crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}**

**pki**

Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.

**export trustpoint**

| `<TRUSTPOINT-NAME>` | Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key
| | • `<TRUSTPOINT-NAME>` – Specify the trustpoint name (should be authenticated).

**<EXPORT-TO-URL>**

Specify the destination address. Both IPv4 and IPv6 address formats are supported. The trustpoint is exported to the address specified here.

**background**

Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on

**passphrase**

| `<KEY-PASSPHRASE>` | Optional. Encrypts the key with a passphrase before exporting
| | • `<KEY-PASSPHRASE>` – Specify the passphrase to encrypt the trustpoint.
| | • background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>pki</strong></td>
<td>Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.</td>
</tr>
<tr>
<td><strong>generate</strong></td>
<td>Generates a certificate and a trustpoint</td>
</tr>
<tr>
<td><strong>self-signed</strong></td>
<td>Generates a self-signed certificate and a trustpoint</td>
</tr>
<tr>
<td><strong>&lt;TRUSTPOINT-NAME&gt;</strong></td>
<td>Specify a name for the certificate and its trustpoint.</td>
</tr>
<tr>
<td>**[generate-rsa-key</td>
<td>use-rsa-key]**</td>
</tr>
<tr>
<td><strong>&lt;RSA-KEYPAIR-NAME&gt;</strong></td>
<td>Specify a name for it. If using an existing RSA Keypair, specify its name.</td>
</tr>
<tr>
<td><strong>autogen-subject-name</strong></td>
<td>Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate.</td>
</tr>
<tr>
<td><strong>email</strong></td>
<td>Optional. Exports the self-signed certificate to a specified e-mail address</td>
</tr>
<tr>
<td><strong>&lt;SEND-TO-EMAIL&gt;</strong></td>
<td>Specify the e-mail address.</td>
</tr>
<tr>
<td><strong>fqdn</strong></td>
<td>Optional. Exports the self-signed certificate to a specified FQDN</td>
</tr>
<tr>
<td><strong>&lt;FQDN&gt;</strong></td>
<td>Specify the FQDN.</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td>Optional. Exports the self-signed certificate to a specified device or system</td>
</tr>
<tr>
<td><strong>&lt;IP&gt;</strong></td>
<td>Specify the device’s IP address.</td>
</tr>
<tr>
<td><strong>on</strong></td>
<td>Optional. Exports the self-signed certificate on a specified device</td>
</tr>
<tr>
<td><strong>&lt;DEVICE-NAME&gt;</strong></td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}**

**pki** Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>generate self-signed</strong></td>
<td>Generates a self-signed certificate and a trustpoint</td>
</tr>
<tr>
<td><strong>&lt;TRUSTPOINT-NAME&gt;</strong></td>
<td>Specify a name for the certificate and its trustpoint.</td>
</tr>
<tr>
<td>**[generate-rsa-key</td>
<td>use-rsa-key]**</td>
</tr>
<tr>
<td><strong>&lt;RSA-KEYPAIR-NAME&gt;</strong></td>
<td>Specify a name for it. If using an existing RSA Keypair, specify its name.</td>
</tr>
</tbody>
</table>
| subject-name <COMMON-NAME> | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate  
| | • <COMMON-NAME> – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length. |
| <COUNTRY> | Sets the deployment country code (2 character ISO code) |
| <STATE> | Sets the state name (2 to 64 characters in length) |
| <CITY> | Sets the city name (2 to 64 characters in length) |
| <ORGANIZATION> | Sets the organization name (2 to 64 characters in length) |
| <ORGANIZATION-UNIT> | Sets the organization unit (2 to 64 characters in length) |
| email <SEND-TO-EMAIL> | Optional. Exports the self-signed certificate to a specified e-mail address  
| | • <SEND-TO-EMAIL> – Specify the e-mail address. |
| fqdn <FQDN> | Optional. Exports the self-signed certificate to a specified FQDN  
| | • <FQDN> – Specify the FQDN. |
| ip-address <IP> | Optional. Exports the self-signed certificate to a specified device or system  
| | • <IP> – Specify the device’s IP address. |

**crypto pki import** [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {on <DEVICE-NAME>}

| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| import | Imports certificates, Certificate Revocation List (CRL), or a trustpoint to the selected device |
| [certificate|crl] <TRUSTPOINT-NAME> | Imports a signed server certificate or CRL  
| | • certificate – Imports signed server certificate  
| | • crl – Imports CRL  
| | • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated). |
| <IMPORT-FROM-URL> | Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported. The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here. |
| background | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on. |
| on <DEVICE-NAME> | The following parameter is recursive and optional:  
| | • on <DEVICE-NAME> – Optional. Performs import operation on a specified device  
| | • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

**crypto pki import trustpoint** <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background|passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}

| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
import
Imports certificates, CRL, or a trustpoint to the selected device

trustpoint
<TRUSTPOINT-NAME>
Imports a trustpoint and its associated CA certificate, server certificate, and private key
• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).

<IMPORT-FROM-URL>
Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported.

background
Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.

passphrase
<KEY-PASSPHRASE>
Optional. Decrypts trustpoint with a passphrase after importing
• <KEY-PASSPHRASE> – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on.
• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on.

on <DEVICE-NAME>
The following parameter is recursive and optional:
• on <DEVICE-NAME> – Optional. Performs import operation on a specified device
• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

• crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {on <DEVICE-NAME>}

pki
Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.

zeroize trustpoint
<TRUSTPOINT-NAME>
Deletes a trustpoint and its associated CA certificate, server certificate, and private key
• <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).

del-key
Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on.

on <DEVICE-NAME>
The following parameter is recursive and optional:
• on <DEVICE-NAME> – Optional. Deletes the trustpoint on a specified device
• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Usage Guidelines
The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:
• IPv4 URLs:
  tftp://<hostname|IP>[:port]/path/file
  ftp://<user>:@<hostname|IP>[:port]/path/file
  sftp://<user>:@<hostname|IP>[:port]/path/file
  http://<hostname|IP>[:port]/path/file
  cf:/path/file
  usb<n>:/path/file
• IPv6 URLs:
  tftp://<hostname|[IPv6]>[:port]/path/file
  ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file
  sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file

Examples
rfs7000-37FABE>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs7000-37FABE>
rfs7000-37FABE>crypto key import rsa test123 url passphrase word background
RSA key import operation is started in background
rfs7000-37FABE>
rfs7000-37FABE>crypto pki generate self-signed word generate-rsa-key word autogen-
subject-name fqdn word
Successfully generated self-signed certificate
rfs7000-37FABE>
rfs7000-37FABE>crypto pki zeroize trustpoint word del-key
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-trustpoint
rfs7000-37FABE>
rfs7000-37FABE>crypto pki authenticate word url background
Import of CA certificate started in background
rfs7000-37FABE>
rfs7000-37FABE>crypto pki import trustpoint word url passphrase word
Import operation started in background
rfs7000-37FABE>

Related Commands

| no | Removes server certificates, trustpoints and their associated certificates |
2.1.9 *crypto-cmp-cert-update*

### User Exec Commands

Triggers a Certificate Management Protocol (CMP) certificate update on a specified device or devices.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}

### Parameters

- **crypto-cmp-cert-update** <TRUSTPOINT-NAME> {on <DEVICE-NAME>}

  *Triggers a CMP certificate update on a specified device or devices*

  - **<TRUSTPOINT-NAME>** — Specify the target trustpoint name. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. Use the crypto-cmp-policy context mode to configure the trustpoint.
  - **on <DEVICE-NAME>** — Optional. Initiates a CMP certificate update and response on a specified device or devices. Specify the name of the AP, wireless controller, or service platform. Multiple devices can be provided as a comma separated list.
  - **<DEVICE-NAME>** — Specify the name of the AP, wireless controller, or service platform.

### Examples

```
rfs4000-229D58>crypto-cmp-cert-update test on B4-C7-99-71-17-28
CMP Cert update success
rfs4000-229D58>
```
### 2.1.10 database

**User Exec Commands**

Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight). Vacuuming a database refers to the process of finding and reclaiming space left over from previous DELETE statements.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
database [drop|repair]
database drop [all|captive-portal|nsight]
database repair {on <DEVICE-NAME>}
```

#### Parameters

- **database drop [all|captive-portal|nsight]**
  - Drops (deletes) all or a specified database
  - `all` — Drops all databases, captive portal and NSight.
  - `captive-portal` — Drops captive-portal database only
  - `nsight` — Drops NSight database only

- **database repair {on <DEVICE-NAME>]**
  - Enables automatic repairing of all databases
  - `on <DEVICE-NAME>` — Optional. Specifies the name of the device hosting the database. When specified, databases on the specified device are periodically checked through to identify and remove obsolete data documents.
  - `<DEVICE-NAME>` — Specify the name of the access point, wireless controller, or service platform.

**Note:** If no device is specified, the system repairs all databases.

#### Examples

```plaintext
nx9500-6C8809>database repair on nx9500-6C8809
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>database-backup</strong></td>
<td>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server</td>
</tr>
<tr>
<td><strong>database-restore</strong></td>
<td>Restores a previously exported database [captive-portal and/or NSight]</td>
</tr>
</tbody>
</table>
### 2.1.11 database-backup

**User Exec Commands**

Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

```
database-backup database [captive-portal|nsight] <URL>
```

**Parameters**

- `database-backup database [captive-portal|nsight] <URL>`

| **database-backup database [captive-portal|nsight]** | Backs up captive portal and/or NSight database to a specified location and file. Select the database to backup:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>captive-portal</strong></td>
<td>Backs up captive portal database</td>
</tr>
<tr>
<td><strong>nsight</strong></td>
<td>Backs up NSight database</td>
</tr>
</tbody>
</table>

After specifying the database type, configure the destination location and file name. The database is backed up at the specified location. Specify the location URL in one of the following formats:

- `ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz`
- `sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz`

**Examples**

```
nx9500-6C8809>database-backup database nsight ftp://anonymous:anonymous@192.168.13.10/backup/backup.tar.gz
```

**Related Commands**

<table>
<thead>
<tr>
<th><strong>database</strong></th>
<th>Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>database-restore</strong></td>
<td>Restores a previously exported (backed up) database [captive-portal and/or NSight]</td>
</tr>
</tbody>
</table>
2.1.12 **database-restore**

*User Exec Commands*

Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored from the backed-up location to the original database.

Supported in the following platforms:

- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

database-restore database [captive-portal|nsight] <URL>

**Parameters**

- database-restore database [captive-portal|nsight] <URL>

| database-restore database [captive-portal|nsight] | Restores previously exported (backed up) captive-portal and/or NSight database. Specify the database type:
| <URL> | Configures the destination location. The database is restored from the specified location. Specify the location URL in one of the following formats:

ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz

**Examples**

```
nx9500-6C8809>database-restore database nsight
ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

**Related Commands**

<table>
<thead>
<tr>
<th>database</th>
<th>Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)</th>
</tr>
</thead>
<tbody>
<tr>
<td>database-backup</td>
<td>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server</td>
</tr>
</tbody>
</table>
2.1.13 **device-upgrade**

*User Exec Commands*

Enables firmware upgrade on an adopted device or a set of adopted devices (access points, wireless controllers, and service platforms). In an *hierarchically managed* (HM) network, this command enables centralized device upgradation across the network.

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

All adopted devices (access points and second-level controllers) are referred to as the 'adoptee'. The adopting devices are the 'adopters'. A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, a controller can either be an adopter (adopts another controller) or an adoptee (is adopted by another controller).

Network administrators can use the device-upgrade command to schedule firmware upgrades across adopted devices within the network. Devices are upgraded based on their device names, MAC addresses, or RF Domain. The firmware image used for the upgrade can either be user-defined or built-in.

The user-defined image is pulled from the defined location and applied to the device(s). Use the `device-upgrade > load-image` command to provide the image file name and location. User-defined images always get precedence over built-in images.

NOC and site controllers possess built-in firmware images for the various device types. If the administrator has not specified an image file name and location, the image on the controller is used to upgrade the device. The following example describes the various scenarios possible in the absence of a user-defined image.

A site controller has been scheduled to upgrade all adopted AP6562s. Before executing the upgrade, the site controller compares the image it possesses with the image on the NOC controller. In case of an image version mismatch, the site controller does the following:

1. If the site controller is a cluster member, it pulls the image:
   - From a cluster peer, provided the AP6562 image version on the peer and the NOC controller matches.
   - From the NOC controller, if the AP6562 image version on the peer and the NOC controller are mismatched.
   - From the NOC controller, if none of the cluster members possess a AP6562 image.
2. If the site controller is not a cluster member, it pulls the image from the NOC controller.

When upgrading devices in a RF Domain, the process is controlled and driven by the NOC controller. For example, in case of a scheduled upgrading of all AP6562s within an *RF Domain*, the NOC controller:

1. Adopts all controllers, in the RF Domain, to the NOC cluster and gets the status of each controller.
2. Upgrades all controllers, in the cluster, without rebooting them.

Once the upgrade is complete, the following two scenarios are possible:

**Scenario 1:** *If the upgrade/reboot options ARE NOT specified by the network administrator, the NOC controller:*

- Pushes the AP6562 image on to the RF Domain manager.
- Reboots the active controller within the RF Domain.
- Reboots standby controllers after the active controller has successfully rebooted.

If the controllers are auto upgrade enabled, all AP6562s are upgraded after the controllers have rebooted and the APs have been re-adopted.

**Scenario 2:** *If the upgrade/reboot options ARE specified by the network administrator, the NOC controller:*

NOTE: Hierarchical management allows the NOC controller to upgrade controllers and access points that are directly or indirectly adopted to it. However, ensure that the NOC controller is loaded with the correct firmware version.
a. Reboots the active controller followed by the standby controllers.
b. Pushes the AP6562 image file on to the RF Domain manager.
c. Initiates upgrades on all AP6562 within the RF Domain.

Ensure the RF Domain controllers are auto upgrade enabled.

NOTE: If the *persist-images* option is selected, the RF Domain manager retains the old firmware image, or else deletes it. For more information on enabling device upgrade on profiles and devices (including the ‘persist-images’ option), see `device-upgrade`.

NOTE: A NOC controller’s capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:

- NOC controller — RFS7000, NX9000, NX95XX (NX9500 and NX9510), NX9600
- Site controller — RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX9000, or NX95XX

Within a HM network, the devices deployed as site controllers depends on the NOC controller device type. For more information on the adoption capabilities of various NOC controller devices, see Usage Guidelines *(NOC controller adoption matrix)*.

NOTE: Standalone devices have to be manually upgraded.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```bash
device-upgrade [<MAC/HOSTNAME>|all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap9000|ap9500|ap9600|ap9900|rf-domain]
```

```bash
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|upgrade-time <TIME>}
```

```bash
device-upgrade all {force|no-reboot/reboot-time <TIME>|upgrade-time <TIME> {no-reboot/reboot-time <TIME>}} {(staggered-reboot)}
```

```bash
device-upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap9000|ap9500|ap9600|ap9900|rf-domain]
```

```bash
device-upgrade cancel-upgrade [-<MAC/HOSTNAME>|all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap9000|ap9500|ap9600|ap9900|rf-domain [-<RF-DOMAIN-NAME>|all]]
```

```bash
device-upgrade load-image [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap9000|ap9500|ap9600|ap9900|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|nx9900|vx9000] {<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}
```
```plaintext
device-upgrade rf-domain [\{<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>\}] [\{all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7552|ap81xx|ap82xx|rf4000|rf6000|rf6500|nx45XX|nx5500|nx65XX|nx75xx|nx9000|nx9600|vx9000\}] \{(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)\}

Parameters

- device-upgrade <MAC/HOSTNAME> \{no-reboot|reboot-time <TIME>|upgrade-time <TIME>\} \{no-reboot|reboot-time <TIME>\}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC/HOSTNAME&gt;</td>
<td>Upgrades firmware on the device identified by the &lt;MAC/HOSTNAME&gt; keyword</td>
</tr>
<tr>
<td>no-reboot</td>
<td>Optional. Enables automatic reboot after a successful upgrade (the device must be manually restarted)</td>
</tr>
<tr>
<td>reboot-time &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic reboot after a successful upgrade</td>
</tr>
<tr>
<td>upgrade-time &lt;TIME&gt;</td>
<td>Optional. Schedules a device firmware upgrade on a specified day and time</td>
</tr>
<tr>
<td>force</td>
<td>Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.</td>
</tr>
<tr>
<td>no-reboot</td>
<td>Optional. Enables automatic reboot after a successful upgrade (the device must be manually restarted)</td>
</tr>
<tr>
<td>reboot-time &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic reboot after a successful upgrade</td>
</tr>
<tr>
<td>upgrade-time &lt;TIME&gt;</td>
<td>Optional. Schedules a device firmware upgrade on all devices on a specified day and time</td>
</tr>
<tr>
<td>staggered-reboot</td>
<td>This keyword is recursive and common to all of the above.</td>
</tr>
</tbody>
</table>
```

- all

  Upgrades firmware on all devices

  ```plaintext
  all \{force|no-reboot|reboot-time <TIME>|upgrade-time <TIME>\} \{no-reboot|reboot-time <TIME>\}\{(staggered-reboot)\}
  ```
**device-upgrade** **<DEVICE-TYPE>** all

Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000.

After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.

**force**

Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.

**no-reboot**

Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)

**reboot-time** **<TIME>**

Optional. Schedules an automatic reboot after a successful upgrade

• **<TIME>** – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

**upgrade-time** **<TIME>**

Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time

• **<TIME>** – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.

The following actions can be performed after a scheduled upgrade:

• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)

• reboot-time **<TIME>** – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

• staggered-reboot

This keyword is recursive and common to all of the above.

• Optional. Enables staggered device reboot (one at a time) without network impact

**cancel-upgrade**

Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades:

• Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames.

• Cancels upgrade on all devices within the network

• Cancels upgrade on all devices of a specific type. Specify the device type.

• Cancels upgrade on specific device(s) or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name.

• cancels a scheduled firmware upgrade on a specified device or on all devices

• `<MAC/HOSTNAME>` – Cancels a scheduled upgrade on the device identified by the `<MAC/HOSTNAME>` keyword. Specify the device’s MAC address or hostname.

• all – Cancels scheduled upgrade on all devices
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel-upgrade &lt;DEVICE-TYPE&gt; all</td>
<td>Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000.</td>
</tr>
</tbody>
</table>
| cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all] | Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains  
  - <RF-DOMAIN-NAME> – Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name.  
  - all – Cancels scheduled device upgrade on all devices across all RF Domains  

- **device-upgrade load-image** [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx500|nx65xx|nx9000|nx9600|vx9000] {<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}

| load-image <DEVICE-TYPE> | Loads device firmware image from a specified location. Use this command to specify the device type and the location of the corresponding image file.  
  - <DEVICE-TYPE> – Specify the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000.  
  After specifying the device type, provide the location of the required device firmware image.  
  - <IMAGE-URL> Specify the device’s firmware image location in one of the following formats:  
    IPv4 URLs:  
    - tftp://<hostname|IP>[:port]/path/file  
    - ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file  
    - sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file  
    - http://<hostname|IP>[:port]/path/file  
    - cf:/path/file  
    - usb<n>:/path/file  
    IPv6 URLs:  
    - tftp://<hostname|[IPv6]>[:port]/path/file  
    - ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file  
    - sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file  

| on <DEVICE-OR-DOMAIN-NAME> | Specify the name of the device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded.  
  - <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.  

- **device-upgrade rf-domain**
  - `<RF-DOMAIN-NAME>`: Upgrades devices in the RF Domain identified by the `<RF-DOMAIN-NAME>` keyword.
  - `all`: Upgrades devices across all RF Domains
  - `containing <WORD>`: Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the `<WORD>` keyword are filtered. Devices on the filtered RF Domains are upgraded.
  - `filter location <WORD>`: Filters devices by their location. All devices with location matching the `<WORD>` keyword are upgraded.

- **<DEVICE-TYPE>**
  - After specifying the RF Domain, select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000.

- **<MAC/HOSTNAME>**
  - Optional. Use this option to identify specific devices for upgradation. Specify the device’s MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.
  - Note: If no MAC address or hostname is specified, all devices of the type selected are upgraded.

- **force**
  - Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.

- **from-controller**
  - Optional. Upgrades a device through the adopted device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.

- **no-reboot**
  - Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)

- **reboot-time <TIME>**
  - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

- **staggered-reboot**
  - This keyword is common to all of the above.
  - Optional. Enables staggered reboot (one at a time) without network impact.
Usage Guidelines (NOC controller adoption matrix)
The following table displays NOC controllers and the corresponding site-level controllers supported by each:

<table>
<thead>
<tr>
<th>Site Controllers supported by each NOC controller</th>
<th>RFS7000</th>
<th>NX9000</th>
<th>NX95XX (NX9500 &amp; NX9510)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFS6000</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFS7000</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>NX45XX</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX65XX</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX7500</td>
<td>-</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>NX9000</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>NX95XX</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

Examples

rfs7000-6DCD4B>show wireless ap configured

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap7131-11E6C4</td>
<td>00-23-68-11-E6-C4</td>
<td>default-ap71xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap8132-711728</td>
<td>B4-C7-99-71-17-28</td>
<td>default-ap81xx</td>
<td>default</td>
<td>00-15-70-81-74-2D</td>
</tr>
<tr>
<td>3</td>
<td>ap81xx-74B45C</td>
<td>B4-C7-99-74-B4-5C</td>
<td>default-ap81xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B>

rfs7000-6DCD4B>device-upgrade ap8132-711728

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-CD-4B</td>
<td>Success</td>
<td>Queued 1 devices to upgrade</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B>

rfs7000-6DCD4B>show device-upgrade status

Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>STATE</th>
<th>UPGRADE TIME</th>
<th>REBOOT TIME</th>
<th>PROGRESS</th>
<th>RETRIES</th>
<th>LAST</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap8132-711728</td>
<td>downloading</td>
<td>immediate</td>
<td>immediate</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>upgrading-devices</td>
<td>immediate</td>
<td>immediate</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following example shows two devices, in the RF domain 'TechPubs' that are adopted to the same controller:

```
rfs6000-6DB5D4> show wireless ap on TechPubs
---------------------------------------------------------------------------------------
                        MODE                  : radio modes - W = WLAN, S=Sensor, ' ' (Space) = radio not present
---------------------------------------------------------------------------------------
------------------------------------------------------------------------ AP-NAME     AP-LOCATION RF-DOMAIN AP-MAC    #RADIOS MODE CLIENT  IPv4        IPv6
------------------------------------------------------------------------ ap6522-43C78C TechPubs.. B4-C7-99-43-C7-8C 2 W-W   0   192.168.13.136  ::
ap6522-57F674 TechPubs.. B4-C7-99-57-F6-74 2 W-W   0   192.168.13.214  ::
------------------------------------------------------------------------
Total number of APs displayed: 2
rfs6000-6DB5D4>
```
Both APs and the controller are running the same image. Therefore, the device-upgrade command fails. This is shown in the following example:

```
rfs6000-6DB5D4>device-upgrade rf-domain TechPubs ap6522
In progress ....
```

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-B5-D4</td>
<td>Fail</td>
<td>TechPubs(Upgrade not required in TechPubs)</td>
</tr>
</tbody>
</table>

```
rfs6000-6DB5D4>
```

Use the ‘force’ parameter to forcefully upgrade the APs.

```
rfs6000-6DB5D4>device-upgrade rf-domain TechPubs ap6522 force
In progress ....
```

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-B5-D4</td>
<td>Success</td>
<td>TechPubs(device type(s) ap6522 added for upgrade),</td>
</tr>
</tbody>
</table>

```
rfs6000-6DB5D4>show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 2
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
```

```
DEVICE    STATE  UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE  ERROR   UPGRADED BY
---------- ------ -------------- -------------- -------------- ----------- -------------- ------ ---------------
ap6522-43C78C waiting immediate immediate 0 0 - rfs6000-6DB5D4
ap6522-57F674 waiting immediate immediate 0 0 - rfs6000-6DB5D4
---------- ------ -------------- -------------- -------------- ----------- -------------- ------ ---------------
rfs6000-6DB5D4>
```

The following examples show the upgradation of devices in a HM network.

**The HM setup is as follows:**

```
rfs7000-6DCD4B (NOC) > l3-adoption > rfs6000-81701D (SITE-CONTROLLER) > l2-adoption > ap8132-711728 (access point)
```

**Step 1: Load AP81XX firmware on the NOC (rfs7000-6DCD4B):**

```
rfs7000-6DCD4B>device-upgrade load-image ap81XX
ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W58/AP81XX-012D.img
```

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs7000-6DCD4B</td>
<td>Success</td>
<td>Successfully initiated load image</td>
</tr>
</tbody>
</table>

```
rfs7000-6DCD4B>
```

```
rfs7000-6DCD4B>show device-upgrade load-image-status
Download of ap81xx firmware file is complete
rfs7000-6DCD4B>
```

```
Step 2: Execute the upgrade command on the NOC. This pushes the AP81XX image through the Site Controller on to the adopted AP81XX (ap8132-711728).

```
rfs7000-6DCD4B>device-upgrade ap8132-711728
--------------------------------------------------------------------------------
CONTROLLER    STATUS                         MESSAGE
--------------------------------------------------------------------------------
B4-C7-99-6D-CD-4B        Success                        Queued 1 devices to upgrade
--------------------------------------------------------------------------------
rfs7000-6DCD4B>show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
---------------------------------------------------------------------------------------
--------------------------
DEVICE          STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE
ERROR    UPGRADED BY
---------------------------------------------------------------------------------------
--------------------------
rfs6000-81701D   downloading         immediate    immediate   95       0       -
rfs6000-81701D
---------------------------------------------------------------------------------------
rfs7000-6DCD4B>show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
---------------------------------------------------------------------------------------
--------------------------
DEVICE             STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE
ERROR   UPGRADED BY
---------------------------------------------------------------------------------------
--------------------------
ap8132-711728    downloading         immediate    immediate   25       0       -
rfs6000-81701D
rfs6000-81701D   upgrading-devices   immediate    immediate   0        0       -
rfs6000-81701D  
---------------------------------------------------------------------------------------
rfs7000-6DCD4B>
```
2.1.14 disable

This command can be executed in the Priv Exec Mode only. This command turns off (disables) the privileged mode command set and returns to the User Executable Mode. The prompt changes from `rfs7000-37FABE#` to `rfs7000-37FABE>`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

disable

Parameters

None

Examples

rfs7000-37FABE#disable
rfs7000-37FABE>
2.1.15 enable

**User Exec Commands**

Turns on (enables) the privileged mode command set. The prompt changes from rfs7000-37FABE> to rfs7000-37FABE#. This command does not do anything in the Privilege Executable mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
enable
```

**Parameters**

None

**Examples**

```plaintext
rfs7000-37FABE>enable
rfs7000-37FABE#
```
2.1.16 file-sync

User Exec Commands

Syncs EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adoptee AP6522/AP6562 client-bridge access points. Use this command to configure parameters that enable syncing of PKCS#12 certificate.

When enabling file syncing, consider the following points:

- The X.509 certificate needs synchronization only if the access point’s radio2, the client-bridge radio, is configured to use EAP-TLS authentication
- Execute the command on the controller adopting the access point
- Ensure that the X.509 certificate file is installed on the controller
- If the adopting device is a site controller with layer 3 adoption to the NOC, ensure that the X.509 certificate is synced across the hierarchically managed setup – between the NOC, site-controller (the staging-controller), and the client-bridge access points.

Syncing of wireless client-bridge certificate can be automated. To automate file syncing, in the controller’s device/profile configuration mode, execute the following command: `file-sync [auto|count <1-20>]`. For more information, see `file-sync`.

For more information on configuring a AP client-bridge, see `bridge`.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
file-sync [cancel|load-file|wireless-bridge]
file-sync cancel wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]
file-sync load-file wireless-bridge <URL>
file-sync wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]
    {from-controller} {reset-radio|upload-time <TIME>}
```

Parameters

- `file-sync cancel wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]` Cancels scheduled wireless client-bridge certificate synchronization on a specified AP, or all APs, or APs within an RF Domain
  - `<DEVICE-NAME>` – Cancels scheduled certificate synchronization on the AP identified by the `<DEVICE-NAME>` parameter. Specify the AP’s hostname or MAC address.
  - all – Cancels scheduled certificate synchronization on all APs
  - rf-domain [<DOMAIN-NAME>|all] – Cancels scheduled certificate synchronization on all APs in a specified RF Domain or in all RF Domains
  - `<DOMAIN-NAME>` – Cancels scheduled certificate synchronization on all APs within the RF Domain identified by the `<DOMAIN-NAME>` parameter. Specify the RF Domain’s name.
  - all – Cancels scheduled certificate synchronization on all RF Domains
• **file-sync load-file wireless-bridge <URL>**

    **file-sync load-file wireless-bridge <URL>**

    Loads the client-bridge certificate to the staging controller. Use this command to load the certificate to the controller before scheduling or initiating a certificate synchronization.
    • <URL> – Provide the certificate location using one of the following formats:
      - tftp://<hostname|IP>[:port]/path/file
      - ftp://<username>:<password>@<hostname|IP>[:port]/path/file
      - sftp://<username>:<password>@<hostname|IP>[:port]/path/file
      - http://<hostname|IP>[:port]/path/file
      - cf:/path/file
      - usb<n>:/path/file
    
    **Note:** Both IPv4 and IPv6 address types are supported.

• **file-sync wireless-bridge [DEVICE-NAME]|all|rf-domain [DOMAIN-NAME]|all} {from-controller}**

    **file-sync wireless-bridge [DEVICE-NAME]|all|rf-domain [DOMAIN-NAME]|all} {from-controller}**

    Configures the following file-sync parameters:
    • post certificate synchronization action
    • upload time
    
    These file-sync options can be applied to a specified AP, all APs, or all APs within a specified RF Domain or on all RF Domains.
    • <DEVICE-NAME> – Applies these parameters to the AP identified by the <DEVICE-NAME> parameter. Specify the AP’s hostname or MAC address.
    • all – Applies these parameters to all APs
    • rf-domain [DOMAIN-NAME]|all – Applies these parameters to all APs in a specified RF Domain or in all RF Domains
      • <DOMAIN-NAME> – Select to apply to APs within the RF Domain identified by the <DOMAIN-NAME> parameter. Specify the RF Domain’s name.
      • all – Select to apply these parameters to all RF Domains
    • from-controller – Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager
    
    After specify the access points to load certificate, specify the following options: reset-radio and upload-time.

**reset-radio**

This keyword is recursive and applicable to all of the above parameters.
Optional. Resets the radio after file synchronization. Reset the radio in case the certificate is renewed along with no changes made to the ‘bridge EAP username’ and ‘bridge EAP password’.

**upload-time <TIME>**

This keyword is recursive and applicable to all of the above parameters.
Optional. Schedules certificate upload at a specified time
• <TIME> – Specify the time in the MM/DD/YYYY-HH:MM or HH:MM format. If no time is configured, the process is initiated as soon as the command is executed.

**Examples**

rfs7000-6DCD4B>file-sync wireless-bridge ap7131-11E6C4 upload-time 12/12/2015-12:30

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-CD-4B</td>
<td>Success</td>
<td>Queued 1 APs to upload</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B>

The following uploads certificate to all access points:

rfs6000-6DB5D4>file-sync wireless-bridge all upload-time 06/05/2015-23:42
### 2.1.17 join-cluster

#### User Exec Commands

Adds a device (access point, wireless controller, or service platform), as a member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
join-cluster <IP> user <USERNAME> password <WORD> {level|mode}
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode [active|standby]}
```

**Parameters**

- `join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode [active|standby]}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>Specify the cluster member's IP address.</td>
</tr>
<tr>
<td>user &lt;USERNAME&gt;</td>
<td>Specify a user account with super user privileges on the new cluster member</td>
</tr>
<tr>
<td>password &lt;WORD&gt;</td>
<td>Specify password for the account specified in the user parameter</td>
</tr>
<tr>
<td>level [1</td>
<td>2]</td>
</tr>
<tr>
<td>mode [active</td>
<td>standby]</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To add a device to an existing cluster:
- Configure a static IP address on the device (access point, wireless controller, or service platform).
- Provide username and password for superuser, network admin, system admin, or operator accounts.

After adding the device to a cluster, execute the “write memory” command to ensure the configuration persists across reboots.

**Examples**

```
rfs7000-37FABE>join-cluster 192.168.13.15 user admin password superuser level 1 mode standby
... connecting to 192.168.13.15
... applying cluster configuration
... committing the changes
... saving the changes
[OK]
rfs7000-37FABE>
```
rfs7000-37FABE>show context
!
! Configuration of RFS7000 version 5.8.1.0-021D
!
! version 2.3
!
.................. .................................................................
interface vlan1
   ip address 192.168.13.15/24
   no ipv6 enable
   no ipv6 request-dhcpv6-options
cluster name TechPubs
cluster mode standby
cluster member ip 192.168.13.15
logging on
logging console warnings
logging buffered warnings
!
end
rfs7000-37FABE>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Initiates cluster context. The cluster context enables centralized management and configuration of all cluster members from any one member.</td>
</tr>
<tr>
<td>create-cluster</td>
<td>Creates a new cluster on a specified device</td>
</tr>
</tbody>
</table>
### 2.1.18 l2tpv3

#### User Exec Commands

Establishes or brings down an *Layer 2 Tunnel Protocol Version 3* (L2TPV3) tunnel

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

- `l2tpv3 tunnel [<TUNNEL-NAME>|all]`
- `l2tpv3 tunnel <TUNNEL-NAME> [down|session|up]`
- `l2tpv3 tunnel <TUNNEL-NAME> down|up [on <DEVICE-NAME>]`
- `l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] [on <DEVICE-NAME>]`
- `l2tpv3 tunnel all [down|up] [on <DEVICE-NAME>]`

#### Parameters

- **l2tpv3 tunnel <TUNNEL-NAME> [down|up] [on <DEVICE-NAME>]**
  - Establishes or brings down L2TPv3 tunnels
  - `<TUNNEL-NAME>` Specifies the tunnel name to establish or bring down
    - `down` – Brings down the specified tunnel
    - `up` – Establishes the specified tunnel
  - `on <DEVICE-NAME>` Optional. Establishes or brings down a tunnel on a specified device
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

- **l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] [on <DEVICE-NAME>]**
  - Establishes or brings down a specified session inside an L2TPv3 tunnel
  - `<TUNNEL-NAME>` – Specify the tunnel name.
    - `session` – Identifies a specific session
    - `<SESSION-NAME>` – Specify the session name.
    - `down` – Brings down the session identified by the `<SESSION-NAME>` keyword
    - `up` – Establishes the session identified by the `<SESSION-NAME>` keyword
  - `on <DEVICE-NAME>` Optional. Establishes or brings down a tunnel session on a specified device
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

- **l2tpv3 tunnel all [down|up] [on <DEVICE-NAME>]**
  - Establishes or brings down all L2TPv3 tunnels
  - `down` – Brings down all tunnels
  - `up` – Establishes all tunnels
<table>
<thead>
<tr>
<th>Optional. Establishes or brings down all tunnels on a specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE>l2tpv3 tunnel Tunnell session TunnellSession1 up on rfs7000-37FABE
```

---

**NOTE:** For more information on the L2TPv3 tunnel configuration mode and commands, see *Chapter 22, L2TPV3-POLICY.*
## 2.1.19 logging

**User Exec Commands**

Modifies message logging settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
logging monitor {<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings}
```

**Parameters**

- `logging monitor {<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings}`

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor</code></td>
<td>Sets the terminal lines logging levels. The logging severity levels can be set from 0-7. The system configures default settings, if no logging severity level is specified.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;0-7&gt;</code> – Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:</td>
</tr>
<tr>
<td></td>
<td>• alerts – Optional. Immediate action needed (severity=1)</td>
</tr>
<tr>
<td></td>
<td>• critical – Optional. Critical conditions (severity=2)</td>
</tr>
<tr>
<td></td>
<td>• debugging – Optional. Debugging messages (severity=7)</td>
</tr>
<tr>
<td></td>
<td>• emergencies – Optional. System is unusable (severity=0)</td>
</tr>
<tr>
<td></td>
<td>• errors – Optional. Error conditions (severity=3)</td>
</tr>
<tr>
<td></td>
<td>• informational – Optional. Informational messages (severity=6)</td>
</tr>
<tr>
<td></td>
<td>• notifications – Optional. Normal but significant conditions (severity=5)</td>
</tr>
<tr>
<td></td>
<td>• warnings – Optional. Warning conditions (severity=4)</td>
</tr>
</tbody>
</table>

**Note:** Before configuring the message logging level, ensure logging module is enabled. To enable message logging, in the device’s configuration mode, execute the `logging > on` command. Message logging can also be enabled on a profile. All devices using the profile will have message logging enabled.

### Examples

```text
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B)#logging on
rfs7000-6DCD4B>logging monitor debugging
rfs7000-6DCD4B>show logging

Logging module: enabled
Aggregation time: disabled
Console logging: level debugging
Monitor logging: disabled
Buffered logging: level warnings
Syslog logging: level warnings
Facility: local7

Log Buffer (103 bytes):

May 17 22:03:53 2015: rfs7000-6DCD4B : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'admin' from 'ssh'
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets terminal lines logging levels</td>
</tr>
</tbody>
</table>
## 2.1.20 mint

### User Exec Commands

Uses MiNT protocol to perform a ping and traceroute to a remote device

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```plaintext
mint ping <MINT-ID> {(count <1-10000>|size <1-64000>|timeout <1-10>)}
mint traceroute <MINT-ID> {(destination-port <1-65535>|max-hops <1-255>|source-port <1-65535>|timeout <1-255>)}
```

### Parameters

- **ping <MINT-ID>***
  - Sends a MiNT echo message to a specified destination
  - `<MINT-ID>` – Specify the destination device’s MiNT ID.
  - **count <1-10000>***
    - Optional. Sets the pings to the MiNT destination
    - `<1- 10000>` – Specify a value from 1 - 10000. The default is 3.
  - **size <1-64000>***
    - Optional. Sets the MiNT payload size in bytes
    - `<1-64000>` – Specify a value from 1 - 64000 bytes. The default is 64 bytes.
  - **timeout <1-10>***
    - Optional. Sets a response time in seconds
    - `<1-10>` – Specify a value from 1 sec - 10 sec. The default is 1 second.

- **traceroute <MINT-ID>***
  - Prints the route packets trace to a device
  - `<MINT-ID>` – Specify the destination device’s MiNT ID.
  - **destination-port <1-65535>***
    - Optional. Sets the Equal-cost Multi-path (ECMP) routing destination port
    - `<1- 65535>` – Specify a value from 1 - 65535. The default port is 45.
  - **max-hops <1-255>***
    - Optional. Sets the maximum number of hops a traceroute packet traverses in the forward direction
    - `<1- 255>` – Specify a value from 1 - 255. The default is 30.
  - **source-port <1-65535>***
    - Optional. Sets the ECMP source port
    - `<1- 65535>` – Specify a value from 1 - 65535. The default port is 45.
  - **timeout <1-255>***
    - Optional. Sets the minimum response time period in seconds
    - `<1- 255>` – Specify a value from 1 sec - 255 sec. The default is 30 seconds.
Examples

rfs7000-37FABE>mint ping 68.22.9D.58 count 5 size 120
MiNT ping 68.22.9D.58 with 120 bytes of data.
  Response from 68.22.9D.58: id=1 time=0.341 ms
  Response from 68.22.9D.58: id=2 time=0.313 ms
  Response from 68.22.9D.58: id=3 time=0.314 ms
  Response from 68.22.9D.58: id=4 time=0.333 ms
  Response from 68.22.9D.58: id=5 time=0.291 ms

--- 68.22.9D.58 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.291/0.318/0.341 ms
rfs7000-37FABE>
2.1.21 no

User Exec Commands

Use the no command to revert a command or to set parameters to their default. This command turns off an enabled feature or reverts settings to default.

NOTE: The commands have their own set of parameters that can be reset.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|virtual-machine|wireless]

no adoption {on <DEVICE-OR-DOMAIN-NAME>}

NOTE: The no > adoption command resets the adoption state of a specified device (and all devices adopted to it) or devices within a specified RF Domain. When executed without specifying the device or RF Domain, the command resets the adoption state of the logged device and all devices, if any, adopted to it.

no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>] {on <DEVICE-OR-DOMAIN-NAME>}

no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>|on <DEVICE-NAME>}}

no logging monitor

no page

no service [block-adopter-config-update|locator|snmp|ssm|wireless]

no service smtp sysoid wing5

no service block-adopter-config-update

no service ssm trace pattern {<WORD>} {on <DEVICE-NAME>}

no service wireless [trace pattern {<WORD>} {on <DEVICE-NAME>}]|unsanctioned ap air-terminate <BSSID> {on <DOMAIN-NAME>}

no service locator {on <DEVICE-NAME>}

no terminal [length|width]

no virtual-machine assign-usb-ports {on <DEVICE-NAME>}

no wireless client [all|<MAC>]

no wireless client all {filter|on}
no wireless client all {filter [wlan <WLAN-NAME>]}

no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}

no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Resets or reverts settings based on the parameters passed |

**Usage Guidelines**

The *no* command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

**Examples**

rfs7000-37FABE>no adoption

rfs7000-37FABE>no page
2.1.22 on

User Exec Commands

Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

on rf-domain [<RF-DOMAIN-NAME>|all]

Parameters

- on rf-domain [<RF-DOMAIN-NAME>|all]

| on rf-domain [<RF-DOMAIN-NAME>|all] | Enters the RF Domain context based on the parameter specified |
|--------------------------------------|----------------------------------------------------------|
| • <RF-DOMAIN-NAME> | Specify the RF Domain name. Enters the specified RF Domain context. |
| • all | Specifies all RF Domains. |

Examples

nx9500-6C8809(rf-domain-all)>?
nx9500-6C8809(rf-domain-all)>on RF-Domain Mode commands:

clearscl | Clears the display screen
| do | Run commands from Exec mode
| end | End current mode and change to EXEC mode
| exit | End current mode and down to previous mode
| help | Description of the interactive help system
| service | Service Commands
| show | Show running system information

nx9500-6C8809(rf-domain-all)>
### 2.1.23 opendns

**User Exec Commands**

Retrieves the OpenDNS device-id from the OpenDNS site

This command integrates access points and controllers with OpenDNS. It obtains the device-id (16 character hex-string) from OpenDNS. This device-id is configured under all WLANs that are to be OpenDNS enabled. When configured and enabled on a WLAN, DNS queries from all wireless clients on the WLAN are redirected to OpenDNS (208.67.220.220 or 208.67.222.222) resolvers. These OpenDNS resolvers act as proxy DNS servers, and also provide additional features, such as Web filtering, performance improvements etc.

**NOTE:** OpenDNS is a free, alternative DNS service that is faster and more reliable than other DNS services available. OpenDNS enables swift navigation of the Web without the outages that are frequent in other ISP provided DNS services. It also blocks inappropriate Web sites, phishing sites, and prevents virus and malware attacks.

**NOTE:** The 'username' and 'password' values passed in this command should be pre-registered with the OpenDNS site. The 'label' can be any value. Only with a combination of a valid 'username', 'password', and any 'label' the OpenDNS server returns a device-id.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```

**Parameters**

- **opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>**
  - **username <USERNAME>** — Configures the OpenDNS user name (should be valid username registered with OpenDNS)
    - `<USERNAME>` – Provide the OpenDNS user name.
  - **password <OPENDNS-PSWD>** — Configures the password associated with the user configured in the previous step
    - `<OPENDNS-PSWD>` – Provide the OpenDNS password for the user.
  - **label <LABEL>** — Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal.
    - `<LABEL>` – Specify your OpenDNS server label.
    - **Note:** For every unique set of username, password, and label only one device-id is returned. Apply this device-id in WLANs that are to be OpenDNS enabled. For information on configuring the device-id in the WLAN context, see `opendns`. 

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Configures the OpenDNS user name (should be valid username registered with OpenDNS)</td>
</tr>
<tr>
<td>password</td>
<td>Configures the password associated with the user configured in the previous step</td>
</tr>
<tr>
<td>label</td>
<td>Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use your OpenDNS credentials to logon to the opendns.org site and use the *labels*, *edit settings*, and *customize content filtering* options to configure Web filtering settings.

Examples

```
ap7131-E6D512>opendns username bob@examplecompany.com password opendns label company_name
Connecting to OpenDNS server...
device_id = 0014AADF8EDC6C59
ap7131-E6D512>
```
2.1.24 page

User Exec Commands

Toggles a device’s paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

page

Parameters

None

Examples

rfs7000-37FABE>page
rfs7000-37FABE>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables device paging</td>
</tr>
</tbody>
</table>
2.1.25 ping

User Exec Commands

Sends Internet Controller Message Protocol (ICMP) echo messages to a user-specified location

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|source [<IP>|pppoe|vlan <1-4094>|wwan]}
```

Parameters

- `<IP/HOSTNAME>` Specify the destination IP address or hostname. When entered without any parameters, this command prompts for an IP address or a hostname.
- `count <1-10000>` Optional. Sets the pings to the specified destination
  - `<1-10000>` – Specify a value from 1 - 10000. The default is 5.
- `dont-fragment {count|size}` Optional. Sets the don’t fragment bit in the ping packet. Packets with the dont-fragment bit specified are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified maximum transmission unit (MTU) value, an error message is sent from the device trying to fragment it.
  - `count <1-10000>` – Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5.
  - `size <1-64000>` – Optional. Sets the ping payload size from 1 - 64000 bytes. The default is 100 bytes.
- `size <1-64000>` Optional. Sets the ping payload size in bytes
  - `<1-64000>` – Specify the ping payload size from 1 - 64000. The default is 100 bytes.
- `source [<IP>|pppoe|vlan <1-4094>|wwan]` Optional. Sets the source address or interface name. This is the source of the ICMP packet to the specified destination.
  - `<IP>` – Specifies the source IP address
  - `pppoe` – Selects the PPP over Ethernet interface
  - `vlan <1-4094>` – Selects the VLAN interface from 1 - 4094
  - `wwan` – Selects the wireless WAN interface
Examples

rfs7000-37FABE>ping 172.16.10.4 count 6
PING 172.16.10.4 (172.16.10.4): 100 data bytes
108 bytes from 172.16.10.4: seq=0 ttl=64 time=0.851 ms
108 bytes from 172.16.10.4: seq=1 ttl=64 time=0.430 ms
108 bytes from 172.16.10.4: seq=2 ttl=64 time=0.509 ms
108 bytes from 172.16.10.4: seq=3 ttl=64 time=0.507 ms
108 bytes from 172.16.10.4: seq=4 ttl=64 time=0.407 ms
108 bytes from 172.16.10.4: seq=5 ttl=64 time=0.402 ms
--- 172.16.10.4 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.402/0.517/0.851 ms
rfs7000-37FABE>

rfs7000-6DCD4B>ping 10.2.0.99 source vlan 1
PING 10.2.0.99 (10.2.0.99) from 172.18.0.2 vlan1: 100(128) bytes of data.
108 bytes from 10.2.0.99: icmp_seq=1 ttl=63 time=1.09 ms
108 bytes from 10.2.0.99: icmp_seq=2 ttl=63 time=0.648 ms
108 bytes from 10.2.0.99: icmp_seq=3 ttl=63 time=0.735 ms
108 bytes from 10.2.0.99: icmp_seq=4 ttl=63 time=0.746 ms
108 bytes from 10.2.0.99: icmp_seq=5 ttl=63 time=0.732 ms
--- 10.2.0.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/mdev = 0.648/0.790/1.091/0.156 ms
rfs7000-6DCD4B>
2.1.26 ping6

User Exec Commands

Sends ICMPv6 echo messages to a user-specified IPv6 address

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ping6 <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}

Parameters

- ping <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPv6/HOSTNAME&gt;</td>
<td>Specify the destination IPv6 address or hostname.</td>
</tr>
<tr>
<td>&lt;INTF-NAME&gt;</td>
<td>Specify the interface name for link local/broadcast address</td>
</tr>
<tr>
<td>count &lt;1-10000&gt;</td>
<td>Optional. Sets the pings to the specified IPv6 destination</td>
</tr>
<tr>
<td>size &lt;1-64000&gt;</td>
<td>Optional. Sets the IPv6 ping payload size in bytes</td>
</tr>
</tbody>
</table>

Usage Guidelines

To configure a device’s IPv6 address, in the VLAN interface configuration mode, use the `ipv6 > address <IPv6-ADDRESS>` command. After configuring the IPv6 address, use the `ipv6 > enable` command to enable IPv6. For more information see, `ipv6`.

Examples

```
rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#show ipv6 interface brief
---------------------------------------------------------------------------------------
INTERFACE          IPV6 MODE  IPV6-ADDRESS/MASK                             TYPE
STATUS   PROTOCOL
---------------------------------------------------------------------------------------
vlan1              True       fe80::223:68ff:fe88:da7/64                    Link-Local
 UP       up
vlan1              True     2001:10:10:10:10:10:10:1/64                 Global-Permanent
 UP       up
vlan2              False      UNASSIGNED                                     None
 UP       up
---------------------------------------------------------------------------------------
rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#
```

```
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=1 ttl=64 time=0.401 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=2 ttl=64 time=0.311 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=3 ttl=64 time=0.309 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=4 ttl=64 time=0.299 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=5 ttl=64 time=0.299 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=6 ttl=64 time=0.313 ms
6 packets transmitted, 6 received, 0% packet loss, time 6999ms
rtt min/avg/max/mdev = 0.299/0.318/0.401/0.031 ms
rfs4000-229D58>
```
2.1.27 ssh

User Exec Commands

Opens a Secure Shell (SSH) connection between two network devices

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}

Parameters

- ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Specify the remote system's IP address or hostname.</td>
</tr>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify the name of the user requesting SSH connection with the remote system.</td>
</tr>
<tr>
<td>&lt;INF-NAME/LINK-LOCAL-ADD&gt;</td>
<td>Optional. Specify the interface's name or link local address.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809>ssh 192.168.13.15 admin
admin@192.168.13.15's password:
rfs7000-37FABE>
2.1.28 telnet

User Exec Commands

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}

Parameters

- telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Configures the destination remote system’s IP (IPv4 or IPv6) address or hostname. The Telnet session is established between the connecting system and the remote system.</td>
</tr>
<tr>
<td></td>
<td>- &lt;IP/HOSTNAME&gt; – Specify the system’s IPv4 or IPv6 address or hostname.</td>
</tr>
<tr>
<td>&lt;TCP-PORT&gt;</td>
<td>Optional. Specify the Transmission Control Protocol (TCP) port number.</td>
</tr>
<tr>
<td>&lt;INTF-NAME&gt;</td>
<td>Optional. Specify the interface name for the link local address.</td>
</tr>
</tbody>
</table>

Examples

nx4500-5CFA8E>telnet 192.168.13.13
Entering character mode
Escape character is '^]'.

NX9500 release 5.8.1.0-027D
nx9500-6C8809 login: admin
Password:
nx9500-6C8809>
2.1.29 terminal

User Exec Commands

Sets the length and width of the CLI display window on a terminal

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
terminal [length|width] <0-512>

Parameters
- terminal [length|width] <0-512>

<table>
<thead>
<tr>
<th>length &lt;0-512&gt;</th>
<th>Sets the number of lines displayed on the terminal window</th>
</tr>
</thead>
<tbody>
<tr>
<td>width &lt;0-512&gt;</td>
<td>Sets the width (the number of characters displayed in one line) of the terminal window</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE>terminal length 150
rfs7000-37FABE>terminal width 215
rfs7000-37FABE>show terminal
Terminal Type: xterm
Length: 150 Width: 215
rfs7000-37FABE>

Related Commands
- no
  Resets the width or length of the terminal window
2.1.30 time-it

User Exec Commands

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

time-it <COMMAND>

Parameters

- time-it <COMMAND>

<table>
<thead>
<tr>
<th>time-it &lt;COMMAND&gt;</th>
<th>Verifies the time taken by a particular command to execute and provide a result</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;COMMAND&gt;</td>
<td>– Specify the command.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE>time-it enable
That took 0.00 seconds..
rfs7000-37FABE#
2.1.31 traceroute

User Exec Commands

Traces the route to a defined destination

Use ‘--help’ or ‘-h’ to display a complete list of parameters for the traceroute command

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

traceroute <LINE>

Parameters

- traceroute <LINE>

tracerrute <LINE> Traces the route to a destination IP address or hostname

• <LINE> – Specify the destination IPv6 address or hostname.

Examples

rfs7000-37FABE>traceroute --help
BusyBox v1.14.1 () multi-call binary


Trace the route to HOST

Options:
- F Set the don't fragment bit
- I Use ICMP ECHO instead of UDP datagrams
- l Display the ttl value of the returned packet
- d Set SO_DEBUG options to socket
- n Print hop addresses numerically rather than symbolically
- r Bypass the normal routing tables and send directly to a host
- v Verbose
- m max_ttl Max time-to-live (max number of hops)
- p port# Base UDP port number used in probes (default is 33434)
- q nqueries Number of probes per 'ttl' (default 3)
- s src_addr IP address to use as the source address
- t tos Type-of-service in probe packets (default 0)
- w wait Time in seconds to wait for a response (default 3 sec)
- g Loose source route gateway (0 max)

rfs7000-37FABE>

rfs7000-6DCD4B>traceroute 192.168.13.16
traceroute to 192.168.13.16 (192.168.13.16), 30 hops max, 38 byte packets
1 192.168.13.16 (192.168.13.16) 5.071 ms 0.294 ms 0.283 ms
rfs7000-6DCD4B>
2.1.32 traceroute6

User Exec Commands

Traces the route to a specified IPv6 destination

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

t traceroute6 <LINE>

Parameters

• traceroute6 <LINE>

| traceroute6 <LINE> | Traces the route to a destination IPv6 address or hostname
|--------------------|---------------------------------------------------|
| <LINE>             | <LINE> – Specify the destination IPv6 address or hostname.

Examples

```
rfs4000-229D58>traceroute6 2001:10:10:10:10:10:10:1
rfs4000-229D58>
```
### 2.1.33 watch

#### User Exec Commands

Repeats the specified CLI command at periodic intervals

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
watch <1-3600> <LINE>
```

#### Parameters

- `watch <1-3600> <LINE>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3600&gt;</td>
<td>Select an interval from 1 - 3600 sec. Pressing CTRL-Z halts execution of the command.</td>
</tr>
<tr>
<td>&lt;LINE&gt;</td>
<td>Specify the CLI command.</td>
</tr>
</tbody>
</table>

#### Examples

```plaintext
rfs7000-6DCD4B>watch 40 ping 192.168.13.16
PING 192.168.13.16 (192.168.13.16) 100(128) bytes of data.
108 bytes from 192.168.13.16: icmp_seq=1 ttl=64 time=0.565 ms
108 bytes from 192.168.13.16: icmp_seq=2 ttl=64 time=0.393 ms
108 bytes from 192.168.13.16: icmp_seq=3 ttl=64 time=0.344 ms
108 bytes from 192.168.13.16: icmp_seq=4 ttl=64 time=0.433 ms
108 bytes from 192.168.13.16: icmp_seq=5 ttl=64 time=0.352 ms
--- 192.168.13.16 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.344/0.417/0.565/0.082 ms

rfs7000-6DCD4B>
```
2.1.34 exit

**User Exec Commands**

Ends the current CLI session and closes the session window

For more information, see `exit`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

exit

**Parameters**

None

**Examples**

rfs7000-37FABE>exit
2.1.35 smart-cache

User Exec Commands

Pre-fetches cached content from the specified list of URLs

Smart caching is a licensed service available on the NX45XX and NX65XX series service platforms. It allows the temporary storage of frequently accessed Web content (Web pages, graphics, audio and video files etc.) on network infrastructure devices. When this content is requested, it is retrieved from a local content cache and not from the origin server. For more information on enabling content caching, see smart-cache-policy.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

smart-cache pre-fetch-immediate <URL-LIST-NAME>

Parameters

- smart-cache pre-fetch-immediate <URL-LIST-NAME>

<table>
<thead>
<tr>
<th>smart-cache</th>
<th>Pre-fetches content from the specified list of URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-fetch-immediate</td>
<td>Provide the URL list names (should be existing and configured). For more information on configuring URL lists, see url-list.</td>
</tr>
</tbody>
</table>

Examples

nx4500-5CFA2B>smart-cache pre-fetch-immediate ?
   URL-LIST  URL List to be Pre Fetched

nx4500-5CFA2B>
## 2.1.36 virtual-machine

### User Exec Commands

Installs, configures, and monitors the status of third-party virtual machines (VMs)

In addition to the WiNG VMs, the NX45XX, NX65XX, NX9500, and NX9510 series service platforms support the installation and administration of third-party VMs. However, the third-party VMs supported by these devices varies.

The third-party VMs supported on NX45XX and NX65XX are:

- TEAM-URC
- TEAM-RLS
- TEAM-VoWLAN

The VM supported on NX9500 and NX9510 is:

- ADSP

Use the virtual-machine command to install the third-party VMs, and configure parameters, such as install media type and location, number of Virtual Central Processing Units (VCPUS), VM memory, VM disk, number of Virtual Network Interfaces (VIFs), and Virtual Networking Computing (VNC) port.

Installing third-party VMs saves on hardware cost and provides a unified VM management interface.

This section is organized into the following sub-sections:

- Syntax **NX45XX, NX65XX**
- Syntax **NX9500 and NX9510**

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax NX45XX, NX65XX**

```plaintext
virtual-machine [assign-usb-ports|console|export|install|restart|set|start|stop|uninstall]

virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}

virtual-machine console [{<VM-NAME>|team-urc|team-rls|team-vowlan}

virtual-machine export <VM-NAME> [{<FILE>|<URL>}{on <DEVICE-NAME>}

virtual-machine install [{<VM-NAME>|team-urc|team-rls|team-vowlan}

virtual-machine install <VM-NAME> type [disk|iso disk-size <SIZE>|vm-archive]
install-media [{<FILE>|<URL>|<USB>}{autostart|memory|on|vcpus|vif-count|vnc}
virtual-machine install [team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine restart [{<VM-NAME>|hard|team-urc|team-rls|team-vowlan}
virtual-machine restart [{<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine restart hard [{<VM-NAME>|team-urc|team-rls|team-vowlan}
virtual-machine set [autostart|memory|vcpus|vif-count|vif-mac|vif-to-vmif|vnc]
virtual-machine set [autostart|ignore|start] memory <512-8192> vcpus <1-4>
vif-count <0-2>vif-mac <VIF-INDEX>{<MAC-INDEX>|<MAC>}
vif-to-vmif <VIF-INDEX>vnc [disable|enable] [{<VM-NAME>|team-urc|team-rls|team-vowlan}
{on <DEVICE-NAME>}

virtual-machine start [{<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine stop [{<VM-NAME>|hard|team-urc|team-rls|team-vowlan]
virtual-machine stop [{<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```
### virtual-machine uninstall

```
virtual-machine uninstall [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

**Parameters** NX45XX, NX65XX

- assign-usb-ports team-vowlan {on <DEVICE-NAME>}

Assigns USB ports to TEAM-VoWLAN

- team-vowlan – Assigns USB ports to TEAM-VoWLAN on a specified device
  - on <DEVICE-NAME> – Optional. Specify the device name.

Use the `no > virtual-machine > assign-usb-ports` command to reassign the port to WING.

**Note:** TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.

### virtual-machine console

```
virtual-machine console [<VM-NAME>|team-urc|team-rls|team-vowlan]
```

Connects to the VM’s console, based on the parameters passed. Select one of the following console options:

- `<VM-NAME>` – Connects to the console of the VM identified by the `<VM-NAME>` keyword. Specify the VM name.
- team-urc – Connects to the VM TEAM Unified Retail Communication’s (URC) (IP-PBX) console
- team-rls – Connects to the VM TEAM Radio Link Service (RLS) server’s console
- team-vowlan – Connects to the VM TEAM-VoWLAN’s (Voice over WLAN) console

### virtual-machine export

```
virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}
```

Exports an existing VM image and settings. Use this command to export the VM to another NX45XX or NX65XX device in the same domain.

- `<VM-NAME>` – Specify the VM name.
- `<FILE>` – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.
- `<URL>` – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path:
  - `tftp://<hostname|IP>[:port]/path/file`
  - `ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`
  - `sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`
  - `http://<hostname|IP>[:port]/path/file`
- on `<DEVICE-NAME>` – Optional. Executes the command on a specified device or devices
  - `<DEVICE-NAME>` – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

The VM should be in a stop state during the export process.

If the destination is a device, the image is copied to a predefined location (VM archive).

### virtual-machine install

```
virtual-machine install <VM-NAME> type [disk|iso disk-size <SIZE>|vm-archive] install-media [<FILE>|<URL>|<USB>] {autostart|memory|on|vcpus|vif-count|vnc}
```

Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process.

- `<VM-NAME>` – Specify the VM name.
  - type – Specify the install-media (image) type. The options are:
    - disk – Specifies the install media type as pre-installed OS disk image (located in the flash memory) Contd..
- iso disk-size \(<\text{SIZE}>\) – Specifies the install media type as ISO file. This is a single file, which contains the OS bootable install media.
- disk-size \(<\text{SIZE}>\) – If the install media type is ISO, specify the disk size in GB.
- vm-archive – Specifies the install media type as VM archive. The VM archive file is a tar.gz file consisting of a pre-installed OS disk image and an associated configuration file. The configuration is a standard libvirt VM template consisting of VM specific information.

**Note:** After specifying the install media type, specify the location of the image. The image can be located in any of the following supported locations: FLASH, USB, or a remote location, such as http, ftp, sftp, tftp.

<table>
<thead>
<tr>
<th>install-media</th>
<th>Specifies the install media location</th>
</tr>
</thead>
</table>
| \(<\text{FILE}>|\<\text{URL}>|\<\text{USB}>>\) \{autostart|memory|on|vcpus|vif-count|vnc\} | \(<\text{FILE}>\) – Specifies the install-media file is located on flash, for example flash:/cache\n\(<\text{URL}>\) – Specifies the install-media file is located on a remote URL. Provide the URL using one of the following formats:
- tftp://\<hostname>|\<IP>[:\port]/\<path>|\<file>
- ftp://\<user>:\<passwd>@\<hostname>|\<IP>[:\port]/\<path>|\<file>
- sftp://\<user>:\<passwd>@\<hostname>|\<IP>[:\port]/\<path>|\<file>
- http://\<hostname>|\<IP>[:\port]/\<path>|\<file>
\(<\text{USB}>\) – Specifies the install-media file is located on a USB. Provide the USB path and file name using the following format:
- usb<n>:/\<path>|\<file>

After specifying the image location, you may provide the following information:
- autostart – Optional. Specifies whether to autostart the VM on system reboot
- ignore – Enables autostart on each system boot/reboot
- start – Disables autostart (default setting)
- memory – Optional. Defines the VM memory size
- \(<512-8192>\) – Specify the VM memory from 512 - 8192 MB. The default is 2048 MB.
- on – Optional. Executes the command on a specified device
- \(<\text{DEVICE-NAME}>\) – Specify the service platform name.
- vcpus – Optional. Specifies the number of VCPUS for this VM
- \(<1-4>\) – Specify the number of VCPUS from 1 - 4. The default setting is 4.
- vif-count – Optional. Configures or resets the VIF number for this VM
- \(<0-2>\) – Specify the VIF number from 0 - 2. The default setting is 1. If assigning a virtual network interface for the VM, optionally specify the following parameters:
- vif-mac – Sets the MAC index for the virtual interfaces 1 & 2.
- vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8. VMIFs are layer 2 interfaces on the WiNG bridge. Each custom VM can have up to a maximum of 2 virtual Ethernet interfaces. By default, these interfaces are internally connected to the Dataplane bridge through VMIF1, which is an untagged port with access VLAN 1.
- vnc – Enables VNC on the virtual interfaces 1 & 2
- vnc – Optional. Disables/enables VNC port. When enabled, provides remote access to VGA through the noVNC client.
- disable – Disables VNC
- enable – Enables VNC (default setting)
### virtual-machine install [team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. Select one of the following options:

- **team-urc** – Installs the VM TEAM-URC image
- **team-rls** – Installs the VM TEAM-RLS image
- **team-vowlan** – Installs the VM TEAM-VoWLAN image

The following keywords are common to all of the above parameters:

- **on <DEVICE-NAME>** – Optional. Executes the command on a specified device or devices
- **<DEVICE-NAME>** – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

### virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

Restarts the VM

- **<VM-NAME>** – Restarts the VM identified by the `<VM-NAME>` keyword
- **team-urc** – Restarts the VM TEAM-URC
- **team-rls** – Restarts the VM TEAM-RLS
- **team-vowlan** – Restarts the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- **on <DEVICE-NAME>** – Optional. Executes the command on a specified device or devices
- **<DEVICE-NAME>** – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

The option 'hard' forces the specified VM to restart.


Configures the VM settings

- **autostart** – Specifies whether to autostart the VM on system reboot
  - **ignore** – Enables autostart on each system reboot
  - **start** – Disables autostart
- **memory** – Defines the VM memory size
  - **<512-8192>** – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.
- **vcpus** – Specifies the number of VCPUS for this VM
  - **<1-4>** – Specify the number of VCPUS from 1 - 4.
- **vif-count** – Configures or resets the VM's VIFs
  - **<0-2>** – Specify the Virtual Interface (VIF) number from 0 - 2.
- **vif-mac** – Configures the MAC address of the selected virtual network interface
  - **<VMIF-INDEX>** – Select the VIF Index from 1 - 2.
  - **<MAC-INDEX>** – Specify the MAC index for the selected VIF from 1 - 8.
  - **<MAC>** – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.

Contd..
Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard l2 ports on the DP bridge, supporting all VLAN and ACL commands. The WiNG software supports up to a maximum of 8 VMIFs. By default, a VM’s interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the `vif-to-vmif` command to map a VIF to a VMIF on the DP bridge.

- `vif-to-vmif` – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.
  - `<VIF-INDEX>` – Selects the VIF index from 1 - 2.
  - `<VMIF-INDEX>` – Specify the VMIF index from 1 - 8.

WiNG provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of the eight VMIF ports for NX4500 and NX6500 service platforms and twelve ports for NX9500 on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.

- `vnc` – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.
  - `disable` – Disables VNC port
  - `enable` – Enables VNC port

After configuring the VM settings, identify the VM to apply the settings.

- `<VM-NAME>` – Applies these settings to the VM identified by the `<VM-NAME>` keyword. Specify the VM name.
- `team-urc` – Applies these settings to the VM TEAM-URC
- `team-rls` – Applies these settings to the VM TEAM-RLS
- `team-vowlan` – Applies these settings to the VM TEAM-VoWLAN
  - `on <DEVICE-NAME>` – Optional. Executes the command on a specified device or devices
  - `<DEVICE-NAME>` – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

<table>
<thead>
<tr>
<th>virtual-machine start [ <code>&lt;VM-NAME&gt;</code></th>
<th>team-urc</th>
<th>team-rls</th>
<th>team-vowlan ] { on <code>&lt;DEVICE-NAME&gt;</code> }</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-machine start</td>
<td>Starts the VM, based on the parameters passed. Select one of the following options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;VM-NAME&gt;</code></td>
<td>• <code>&lt;VM-NAME&gt;</code> – Starts the VM identified by the <code>&lt;VM-NAME&gt;</code> keyword. Specify the VM name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>team-urc</td>
<td>• <code>team-urc</code> – Starts the VM TEAM-URC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>team-rls</td>
<td>• <code>team-rls</code> – Starts the VM TEAM-RLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>team-vowlan</td>
<td>• <code>team-vowlan</code> – Starts the VM TEAM-VoWLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Contd..</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following keywords are common to all of the above parameters:
- on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
- <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**virtual-machine stop** [ <VM-NAME> | hard | team-urc | team-rls | team-vowlan ] { on <DEVICE-NAME> }

Stops the VM, based on the parameters passed. Select one of the following options:
- <VM-NAME> – Stops the VM identified by the <VM-NAME> keyword. Specify the VM name.
- team-urc – Stops the VM TEAM-URC
- team-rls – Stops the VM TEAM-RLS
- team-vowlan – Stops the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:
- on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
- <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

The option ‘hard’ forces the selected VM to shutdown.

**virtual-machine uninstall** [ <VM-NAME> | team-urc | team-rls | team-vowlan ] { on <DEVICE-NAME> }

Uninstalls the specified VM
- <VM-NAME> – Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name.
- team-urc – Uninstalls the VM TEAM-URC
- team-rls – Uninstalls the VM TEAM-RLS
- team-vowlan – Uninstalls the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:
- on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
- <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**Note:** This command releases the VM’s resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system.

**Syntax NX9500 and NX9510**

```
virtual-machine console adsp
virtual-machine install [adsp] { on <DEVICE-NAME> }
virtual-machine restart [adsp] { on <DEVICE-NAME> }
virtual-machine set disk-size <100-500> adsp { on <DEVICE-NAME> }
virtual-machine set memory <512-8192> adsp { on <DEVICE-NAME> }
virtual-machine set wing-memory <12288-32739>
virtual-machine [start|stop] adsp { on <DEVICE-NAME> }
virtual-machine uninstall adsp { on <DEVICE-NAME> }
```

**NOTE:** On an NX95XX, you can use the install, start, stop, restart, and set commands to manage a third-party VM running on a NX45XX and NX65XX. You can also configure a third-party VM’s settings through a NX95XX series service platform.
### Parameters NX9500 and NX9510

- **virtual-machine console adsp**

  Connects to the *Air-Defense Services Platform* (ADSP) VM’s management console. When ADSP is running on the NX9500 and NX9510 model service platforms, WiNG communicates with ADSP using a *single sign-on* (SSO) authentication mechanism. Once the user is logged in, WiNG gains access to ADSP without being prompted to login again at ADSP. However, the WiNG and ADSP databases are not synchronized. ADSP has its own user database, stored locally within its VM, which is accessed whenever a user logs directly into ADSP.

  WiNG and ADSP must be consistent in the manner events are reported up through a network hierarchy to ensure optimal interoperability and event reporting. To provide such consistency, WiNG has added support for an ADSP-like hierarchal tree. The tree resides within WiNG, and ADSP reads it from WiNG and displays the network hierarchy in its own ADSP interface. The hierarchal tree can also be used to launch ADSP modules (like Spectrum Analyzer) directly from WiNG. For more information on configuring WiNG tree-node structure, see *tree-node*.

- **virtual-machine install adsp {on <DEVICE-NAME>]**

  Installs the ADSPVM
  - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

  Before installing the ADSP VM, execute the upgrade command, giving the path and file name of the ADSP firmware image. This extracts the image on to the device (NX9500 or NX9510) on which the command has been executed. On successful completion of this process, execute the reload command to reboot the device. Once the device has been successfully rebooted, execute the `virtual-machine > install > adsp` command.

  For example:

  ```
  #upgrade tftp://20.1.1.60/adsp-9.1.1
  May 29 15:12:41 2015: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 192 "-" "-
  03-5.8.1.0-008D.img
  May 29 15:12:51 2014: nx9500-6C874D : %DIAG-6-NEW_LED_STATE: LED state message FIRMWARE_UPGRADE_STARTED from module led_msg
  Running from partition /dev/sda8
  Validating image file header
  Extracting files (this may take some time).....May 29 15:12:53 2014: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 923 "-" "-
  ...........
  ```

- **virtual-machine restart adsp {on <DEVICE-NAME>]**

  Restarts the ADSP VM
  - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
### virtual-machine set disk-size \(<100-500>\) adsp \{on \(<\text{DEVICE-NAME}\>)\}

Sets the ADSP VM's disk size (in GB).
- \(<100-500>\) – Specify a value from 100 - 500 GB.
- adsp – Sets the VM as ADSP
  - on \(<\text{DEVICE-NAME}\>) – Optional. Executes the command on a specified device or devices
  - \(<\text{DEVICE-NAME}\>) – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

Stop the ADSP VM before executing this command.

### virtual-machine set memory \(<512-8192>\) adsp \{on \(<\text{DEVICE-NAME}\>)\}

Modifies the ADSP VM's memory
- \(<512-8192>\) – Specify a value from 512 - 8192 MB.
- adsp – Sets the VM as ADSP
  - on \(<\text{DEVICE-NAME}\>) – Optional. Executes the command on a specified device or devices
  - \(<\text{DEVICE-NAME}\>) – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

### virtual-machine set wing-memory \(<12288-32739>\)

Specifies the WiNG memory size in MB
This command is applicable only to the NX9500 and NX9510 service platforms. Use the `show > virtual-machine-configuration` command to view the configured memory allocation. Use the `show > virtual-machine-statistics` to view the current allocated memory allocation.
- \(<12288-32739>\) – Specify a value from 12288 - 32739 MB. The default is 18432 MB.

The new memory setting takes effect only after the next boot.

### virtual-machine \([\text{start|stop}]\) adsp \{on \(<\text{DEVICE-NAME}\>)\}

Starts/stops the ADSP VM
- start – Starts the ADSP VM. Use this command to boot a shut down VM (in a stop state).
- stop – Stops a running ADSP VM. Use this command to shut down a running VM.
  - on \(<\text{DEVICE-NAME}\>) – Optional. Executes the start/stop command on a specified device or devices
  - \(<\text{DEVICE-NAME}\>) – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

### virtual-machine uninstall adsp \{on \(<\text{DEVICE-NAME}\>)\}

Uninstalls the ADSP VM
- adsp – Sets the VM as ADSP
  - on \(<\text{DEVICE-NAME}\>) – Optional. Executes the command on a specified device or devices
  - \(<\text{DEVICE-NAME}\>) – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
Examples
The following examples show the VM installation process:

Installation media: USB

<DEVICE>>virtual-machine install <VM-NAME> type iso disk-size 8 install-media usb1://vms/win7.iso autostart start memory 512 vcpus 3 vif-count 2 vnc enable

Installation media: pre-installed disk image

<DEVICE>>virtual-machine install <VM-NAME> type disk install-media flash:/vms/win7_disk.img autostart start memory 512 vcpus 3 vif-count 2 vnc-enable on <DEVICE-NAME>

In the preceding example, the command is executed on the device identified by the <DEVICE-NAME> keyword. In such a scenario, the disk-size is ignored if specified. The VM has the install media as first boot device.

Installation media: VM archive

<DEVICE>>virtual-machine install type vm-archive install-media flash:/vms/<VM-NAME> vcpus 3

In the preceding example, the default configuration attached with the VM archive overrides any parameters specified.

Exporting an installed VM:

<DEVICE>>virtual-machine export <VM-NAME> <URL> on <DEVICE-NAME>

In the preceding example, the command copies the VM archive on to the URL (VM should be in stop state).

nx4500-5CFA2B>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
nx4500-5CFA2B>

NOTE: Use the show > virtual-machine > [configuration|debugging|export|statistics] command to view installed VM details.

Related Commands

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reassigns USB port to WiNG</td>
</tr>
</tbody>
</table>
Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the hostname of the device followed by a pound sign (#).

To access the PRIV EXEC mode, enter the following at the prompt:

<DEVICE>>enable
<DEVICE>#

The PRIV EXEC mode is often referred to as the enable mode, because the enable command is used to enter the mode.

There is no provision to configure a password to get direct access to PRIV EXEC (enable) mode.

<DEVICE>##?

Privileged command commands:

- **archive**: Manage archive files
- **boot**: Boot commands
- **captive-portal-page-upload**: Captive portal advanced page upload
- **cd**: Change current directory
- **change-passwd**: Change password
- **clear**: Clear
- **clock**: Configure software system clock
- **cluster**: Cluster commands
- **commit**: Commit all changes made in this session
- **configure**: Enter configuration mode
- **connect**: Open a console connection to a remote device
- **copy**: Copy contents of one dir to another
- **cpe**: T5 CPE configuration
- **create-cluster**: Create a cluster
- **crypto**: Encryption related commands
- **crypto-cmp-cert-update**: Update the cmp certs
- **database**: Database
- **database-backup**: Backup database
- **database-restore**: Restore database
- **debug**: Debugging functions
- **delete**: Deletes specified file from the system
- **device-upgrade**: Device firmware upgrade
- **diff**: Display differences between two files
- **dir**: List files on a filesystem
- **disable**: Turn off privileged mode command
- **edit**: Edit a text file
- **enable**: Turn on privileged mode command
- **erase**: Erase a filesystem
ex3500                      EX3500 commands
factory-reset               Factory reset configuration and reload
file-sync                   File sync between controller and adoptees
format                      Format file system
halt                        Halt the system
help                        Description of the interactive help system
join-cluster                Join the cluster
l2tpv3                      L2tpv3 protocol
logging                     Modify message logging facilities
mint                        MiNT protocol
mkdir                       Create a directory
more                        Display the contents of a file
no                          Negate a command or set its defaults
on                          On RF-Domain
opendns                     Opendns username/password configuration
page                        Toggle paging
ping                        Send ICMP echo messages
ping6                       Send ICMPv6 echo messages
pwd                         Display current directory
raid                        RAID operations
re-elect                    Perform re-election
reload                      Halt and perform a warm reboot
remote-debug                Troubleshoot remote system(s)
rename                      Rename a file
revert                      Revert changes
rmdir                       Delete a directory
self                        Configure context of the device currently logged into
service                     Service Commands
show                        Show running system information
smart-cache                 Content Cache Operation
ssh                         Open an ssh connection
t5                          T5 commands
telnet                      Open a telnet connection
terminal                    Set terminal line parameters
time-it                     Check how long a particular command took between request and completion of response
traceroute                  Trace route to destination
traceroute6                 Trace route to destination(IPv6)
upgrade                     Upgrade software image
upgrade-abort               Abort an ongoing upgrade
virtual-machine             Virtual Machine
watch                       Repeat the specific CLI command at a periodic interval
write                       Write running configuration to memory or terminal
clrscr                      Clears the display screen
exit                        Exit from the CLI

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character.
## 3.1 Privileged Exec Mode Commands

The following table summarizes the PRIV EXEC Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Manages file archive operations</td>
<td>page 3-6</td>
</tr>
<tr>
<td>boot</td>
<td>Specifies the image used after reboot</td>
<td>page 3-8</td>
</tr>
<tr>
<td>captive-portal-page-upload</td>
<td>Uploads captive portal advanced pages</td>
<td>page 3-9</td>
</tr>
<tr>
<td>cd</td>
<td>Changes the current directory</td>
<td>page 3-12</td>
</tr>
<tr>
<td>change-passwd</td>
<td>Changes the password of a logged user</td>
<td>page 3-13</td>
</tr>
<tr>
<td>clear</td>
<td>Clears parameters, cache entries, table entries, and other similar entries</td>
<td>page 3-14</td>
</tr>
<tr>
<td>clock</td>
<td>Configures the system clock</td>
<td>page 3-27</td>
</tr>
<tr>
<td>cluster</td>
<td>Initiates a cluster context</td>
<td>page 3-28</td>
</tr>
<tr>
<td>configure</td>
<td>Enters the global configuration mode</td>
<td>page 3-29</td>
</tr>
<tr>
<td>connect</td>
<td>Begins a console connection to a remote device</td>
<td>page 3-30</td>
</tr>
<tr>
<td>copy</td>
<td>Copies a file from any location to the wireless controller, service platform, or access point</td>
<td>page 3-31</td>
</tr>
<tr>
<td>cpe</td>
<td>Enables a WiNG controller to perform certain operations on an adopted T5 Customer Premises Equipment (CPE) device. This command is specific to the RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX9XXX devices.</td>
<td>page 3-32</td>
</tr>
<tr>
<td>create-cluster</td>
<td>Creates a new cluster on a specified device</td>
<td>page 3-34</td>
</tr>
<tr>
<td>crypto</td>
<td>Enables encryption</td>
<td>page 3-36</td>
</tr>
<tr>
<td>crypto-cmp-cert-update</td>
<td>Triggers a CMP certificate update on a specified device or devices</td>
<td>page 3-45</td>
</tr>
<tr>
<td>database</td>
<td>Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)</td>
<td>page 3-46</td>
</tr>
<tr>
<td>database-backup</td>
<td>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server</td>
<td>page 3-47</td>
</tr>
<tr>
<td>database-restore</td>
<td>Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored to the original database.</td>
<td>page 3-48</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a specified file from the system</td>
<td>page 3-49</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade parameters</td>
<td>page 3-50</td>
</tr>
<tr>
<td>diff</td>
<td>Displays the differences between two files</td>
<td>page 3-57</td>
</tr>
<tr>
<td>dir</td>
<td>Displays the list of files on a file system</td>
<td>page 3-58</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the privileged mode command set</td>
<td>page 3-59</td>
</tr>
</tbody>
</table>
### Table 3.1 Privileged Exec Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit</td>
<td>Edits a text file</td>
<td>page 3-60</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on (enables) the privileged mode commands set</td>
<td>page 3-61</td>
</tr>
<tr>
<td>erase</td>
<td>Erases a file system</td>
<td>page 3-62</td>
</tr>
<tr>
<td>ex3500</td>
<td>Enables EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP related configurations.</td>
<td>page 3-64</td>
</tr>
<tr>
<td>factory-reset</td>
<td>Erases startup configuration on a specified device or all devices within a specified RF Domain</td>
<td>page 3-71</td>
</tr>
<tr>
<td>file-sync</td>
<td>Configures parameters enabling syncing of PKCS#12 certificate between the staging-controller and adoptee AP6522/AP6562 client-bridge access points</td>
<td>page 3-75</td>
</tr>
<tr>
<td>format</td>
<td>Formats a device's compact flash file system</td>
<td>page 3-77</td>
</tr>
<tr>
<td>halt</td>
<td>Halts a device (access point, wireless controller, or service platform)</td>
<td>page 3-78</td>
</tr>
<tr>
<td>join-cluster</td>
<td>Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices</td>
<td>page 3-79</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Establishes or brings down Layer 2 Tunneling Protocol Version 3 (L2TPV3) tunnels</td>
<td>page 3-81</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging parameters</td>
<td>page 3-83</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocols</td>
<td>page 3-85</td>
</tr>
<tr>
<td>mkdir</td>
<td>Creates a new directory in the file system</td>
<td>page 3-87</td>
</tr>
<tr>
<td>more</td>
<td>Displays the contents of a file</td>
<td>page 3-88</td>
</tr>
<tr>
<td>no</td>
<td>Reverts a command or sets values to their default</td>
<td>page 3-89</td>
</tr>
<tr>
<td>on</td>
<td>Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, show</td>
<td>page 3-91</td>
</tr>
<tr>
<td>opendns</td>
<td>Connects to the OpenDNS site using OpenDNS registered credentials (username, password) to obtain the device-id. This command is a part of the process integrating access points and controllers with the OpenDNS service.</td>
<td>page 3-92</td>
</tr>
<tr>
<td>page</td>
<td>Toggles a device’s (access point, wireless controller, or service platform) paging function</td>
<td>page 3-94</td>
</tr>
<tr>
<td>ping</td>
<td>Sends ICMP echo messages to a user-specified location</td>
<td>page 3-95</td>
</tr>
<tr>
<td>ping6</td>
<td>Sends ICMPv6 echo messages to a user-specified location</td>
<td>page 3-97</td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current directory</td>
<td>page 3-98</td>
</tr>
<tr>
<td>re-elect</td>
<td>Re-elects the tunnel controller (wireless controller, service platform, or access point)</td>
<td>page 3-99</td>
</tr>
<tr>
<td>reload</td>
<td>Halts a device (wireless controller, service platform, or access point) and performs a warm reboot</td>
<td>page 3-100</td>
</tr>
</tbody>
</table>
### Table 3.1 Privileged Exec Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rename</code></td>
<td>Renames a file in the existing file system</td>
<td>page 3-105</td>
</tr>
<tr>
<td><code>rmdir</code></td>
<td>Deletes an existing file from the file system</td>
<td>page 3-106</td>
</tr>
<tr>
<td><code>self</code></td>
<td>Displays the configuration context of the device</td>
<td>page 3-107</td>
</tr>
<tr>
<td><code>ssh</code></td>
<td>Connects to another device using a secure shell</td>
<td>page 3-108</td>
</tr>
<tr>
<td><code>t5</code></td>
<td>Executes the following operations on a T5 device: copy, rename, delete, and</td>
<td>page 3-109</td>
</tr>
<tr>
<td></td>
<td>write. This command is specific to the RFS4000, RFS6000, RFS7000, NX45XX,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NX65XX, NX9XXX devices.</td>
<td></td>
</tr>
<tr>
<td><code>telnet</code></td>
<td>Opens a Telnet session</td>
<td>page 3-111</td>
</tr>
<tr>
<td><code>terminal</code></td>
<td>Sets the length and width of the terminal window</td>
<td>page 3-112</td>
</tr>
<tr>
<td><code>time-it</code></td>
<td>Verifies the time taken by a particular command between request and</td>
<td>page 3-113</td>
</tr>
<tr>
<td></td>
<td>response</td>
<td></td>
</tr>
<tr>
<td><code>traceroute</code></td>
<td>Traces the route to a defined destination</td>
<td>page 3-114</td>
</tr>
<tr>
<td><code>traceroute6</code></td>
<td>Sends ICMPv6 echo messages to a user-specified location</td>
<td>page 3-115</td>
</tr>
<tr>
<td><code>upgrade</code></td>
<td>Upgrades the software image</td>
<td>page 3-116</td>
</tr>
<tr>
<td><code>upgrade-abort</code></td>
<td>Abort an ongoing software image upgrade</td>
<td>page 3-120</td>
</tr>
<tr>
<td><code>watch</code></td>
<td>Repeats a specified CLI command at a periodic interval</td>
<td>page 3-121</td>
</tr>
<tr>
<td><code>smart-cache</code></td>
<td>Pre-fetches content cache from the specified list of URLs. This command is</td>
<td>page 3-123</td>
</tr>
<tr>
<td></td>
<td>specific to the NX45XX and NX65XX series service platforms.</td>
<td></td>
</tr>
<tr>
<td><code>virtual-machine</code></td>
<td>Installs, configures, and monitors the status of virtual machines (VMs).</td>
<td>page 3-124</td>
</tr>
<tr>
<td></td>
<td>This command is specific to the NX45XX, NX65XX, NX9500, NX9510, and NX9600</td>
<td></td>
</tr>
<tr>
<td></td>
<td>series service platforms.</td>
<td></td>
</tr>
<tr>
<td><code>raid</code></td>
<td>Enables RAID management. This command is specific to the NX9500</td>
<td>page 3-133</td>
</tr>
<tr>
<td></td>
<td>series service platforms.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.

**NOTE:** The input parameter `<HOSTNAME>`, if used in syntaxes across this chapter, cannot include an underscore (_) character.
### 3.1.1 archive

#### Privileged Exec Mode Commands

Manages file archive operations

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive tar /table [&lt;FILE&gt;</td>
<td>&lt;URL&gt;]</td>
</tr>
<tr>
<td>archive tar /create [&lt;FILE&gt;</td>
<td>&lt;URL&gt;] &lt;FILE&gt;</td>
</tr>
<tr>
<td>archive tar /xtract [&lt;FILE&gt;</td>
<td>&lt;URL&gt;] &lt;DIR&gt;</td>
</tr>
</tbody>
</table>

#### Parameters

- **archive tar /table [<FILE>|<URL>]**
  - `<FILE>` Defines a tar filename
  - `<URL>` Sets the tar file URL

- **archive tar /create [<FILE>|<URL>] <FILE>**
  - `<FILE>` Defines tar filename
  - `<URL>` Sets the tar file URL

- **archive tar /xtract [<FILE>|<URL>] <DIR>**
  - `<DIR>` Specify a directory name. When used with /create, dir is the source directory for the tar file. When used with /xtract, dir is the destination file where contents of the tar file are extracted.
Examples

Following examples show how to zip the folder flash:/log/?

nx9500-6C8809# dir flash: /
Directory of flash: /

drwx             Tue Mar 17 07:01:39 2015   crashinfo
drwx             Thu May 16 09:29:10 2013   upgrade
drwx             Tue Mar 17 09:53:15 2015   log
drwx             Wed Mar 18 06:27:08 2015 archived_logs
drwx             Thu May 16 09:29:10 2013 cache
drwx             Thu Feb 19 08:53:45 2015   floorplans
drwx             Mon Sep 15 03:40:02 2014   hotspot

nx9500-6C8809#

nx9500-6C8809# archive tar /create flash:/in.tar flash:/log/
log/ log/adopts.log.2
log/user_reg_report-426543113.csv
log/dpd2.log
log/mart_websock_server.log
log/nuxi/
log/nuxi/beanyaml.log
log/nuxi/statsreqresp.1.log
log/nuxi/hadoop.log.2014-08-03
log/nuxi/puts.log
log/nuxi/copy2w.log
log/nuxi/obj2yaml.log
log/nuxi/infl.log
log/nuxi/copy2mb.log
log/nuxi/amf.log
--More--

nx9500-6C8809#

nx9500-6C8809# dir flash: /
Directory of flash: /

drwx             Tue Mar 17 07:01:39 2015   crashinfo
drwx             Thu May 16 09:29:10 2013   upgrade
drwx             Tue Mar 17 09:53:15 2015   log
drwx             Wed Mar 18 06:34:08 2015 archived_logs
drwx             Thu May 16 09:29:10 2013 cache
drwx             Thu Feb 19 08:53:45 2015   floorplans
-rw- 29708288  Wed Mar 18 06:32:13 2015   in.tar
drwx             Mon Sep 15 03:40:02 2014   hotspot

nx9500-6C8809#
3.1.2 boot

Privileged Exec Mode Commands

Specifies the image used after reboot

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`boot system [primary|secondary] {on <DEVICE-NAME>}`

Parameters

- `boot system [primary|secondary] {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system [primary</td>
<td>secondary]</td>
</tr>
<tr>
<td></td>
<td>- primary — Uses the primary image after reboot</td>
</tr>
<tr>
<td></td>
<td>- secondary — Uses the secondary image after reboot</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Specifies the primary or secondary image location on a specified device</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-NAME&gt; — Specify the name of the AP, wireless controller, or service platform</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809# show boot
-----------------------------
IMAGE     | BUILD DATE     | INSTALL DATE     | VERSION          
-----------------------------
Primary   | 03/31/2015 05:54:02 | 03/31/2015 08:42:04 | 5.8.1.0-025D     
Secondary | 04/14/2015 03:48:55 | 04/16/2015 08:45:03 | 5.8.1.0-027D     
-----------------------------
Current Boot : Secondary 
Next Boot : Secondary 
Software Fallback : Enabled 
VM support : Present 
nx9500-6C8809# 

nx9500-6C8809# boot system primary
Updated system boot partition
nx9500-6C8809# 

nx9500-6C8809# show boot
-----------------------------
IMAGE     | BUILD DATE     | INSTALL DATE     | VERSION          
-----------------------------
Primary   | 03/31/2015 05:54:02 | 03/31/2015 08:42:04 | 5.8.1.0-025D     
Secondary | 04/14/2015 03:48:55 | 04/16/2015 08:45:03 | 5.8.1.0-027D     
-----------------------------
Current Boot : Secondary 
Next Boot : Primary 
Software Fallback : Enabled 
VM support : Present 
nx9500-6C8809# 
```
3.1.3 captive-portal-page-upload

Privileged Exec Mode Commands

Uploads captive portal advanced pages to connected access points. Use this command to provide connected access points with specific captive portal configurations so they can successfully provision login, welcome, and condition pages to requesting clients attempting to access the wireless network using the captive portal.

NOTE: Ensure that the captive portal pages to be uploaded are *.tar files.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
captive-portal-page-upload [<CAPTIVE-PORTAL-NAME>|cancel-upload|delete-file|load-file]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME]|all|rf-domain]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME]|all]
    {upload-time <TIME>}
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME]|all]
    {from-controller} {(upload-time <TIME>)}
captive-portal-page-upload cancel-upload [<MAC/HOSTNAME]|all|on rf-domain
    [<DOMAIN-NAME]|all]]
captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>
captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

Parameters

- captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME]|all]
  {upload-time <TIME>}

  captive-portal-page-upload <CAPTIVE-PORTAL-NAME>
  Uploads advanced pages specified by the <CAPTIVE-PORTAL-NAME> parameter
  • <CAPTIVE-PORTAL-NAME> – Specify captive portal name (should be existing and configured).

  <MAC/HOSTNAME>
  Uploads to a specified AP
  • <MAC/HOSTNAME> – Specify the AP’s MAC address or hostname.

  all
  Uploads to all APs

  upload-time <TIME>
  Optional. Schedules an upload time
  • <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal-page-upload</td>
<td>Uploads advanced pages specified by the <code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> parameter</td>
</tr>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code></td>
<td>• <code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> – Specify captive portal name (should be existing and configured).</td>
</tr>
<tr>
<td>rf-domain</td>
<td>Uploads to all APs within a specified RF Domain or all RF Domains</td>
</tr>
<tr>
<td>`[&lt;DOMAIN-NAME&gt;</td>
<td>all]`</td>
</tr>
<tr>
<td>from-controller</td>
<td>Optional. Uploads to APs from the adopted device</td>
</tr>
<tr>
<td>upload-time <code>&lt;TIME&gt;</code></td>
<td>Optional. Schedules an AP upload</td>
</tr>
<tr>
<td>cancel-upload</td>
<td>Cancels a scheduled AP upload</td>
</tr>
<tr>
<td>`[&lt;MAC/HOSTNAME&gt;</td>
<td>all</td>
</tr>
<tr>
<td>delete-file</td>
<td>Deletes a captive portal's uploaded captive-portal internal page files</td>
</tr>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> <code>&lt;FILE-NAME&gt;</code></td>
<td>• <code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> – Specify the captive portal’s name.</td>
</tr>
<tr>
<td>load-file</td>
<td>Loads captive-portal advanced pages</td>
</tr>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> <code>&lt;URL&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>
<CAPTIVE-PORTAL-NAME> <URL>

Specify captive portal name (should be existing and configured) and location.

- <URL> – Specifies location of the captive-portal's advanced pages. Use one of the following formats:

IPv4 URLs:
- `tftp://<hostname|IP>[:port]/path/file`
- `ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`
- `sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`
- `http://<hostname|IP>[:port]/path/file`
- `cf:/path/file`
- `usb<n>:/path/file`

IPv6 URLs:
- `tftp://<hostname|IPv6>[:port]/path/file`
- `ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file`
- `sftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file`
- `http://<hostname|IPv6>[:port]/path/file`

**Note:** The captive portal pages are downloaded to the controller from the location specified here. After downloading use the `captive-portal-page-upload` <CAPTIVE-PORTAL-NAME> > <DEVICE-OR-DOMAIN-NAME> command to upload these pages to APs.

**Examples**

```
ap6562-B1A214#captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/pages_new_only.tar
ap6562-B1A214#
ap6562-B1A214#show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214#
ap6562-B1A214#captive-portal-page-upload captive_portal_test all
```

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-0A-81-B1-A2-14</td>
<td>Success</td>
<td>Added 6 APs to upload queue</td>
</tr>
</tbody>
</table>

```
ap6562-B1A214#show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0
```

```
ap6562-B1A738 downloading immediate 100 0 - None
```
3.1.4 cd

Privileged Exec Mode Commands

Changes the current directory

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
cd {<DIR>}
```

Parameters

- `cd {<DIR>}`

<table>
<thead>
<tr>
<th><code>&lt;DIR&gt;</code></th>
<th>Optional. Changes the current directory to the directory identified by the <code>&lt;DIR&gt;</code> keyword. If a directory name is not provided, the system displays the current directory.</th>
</tr>
</thead>
</table>

Examples

```
rfs7000-37FABE#cd flash:/log/
rfs7000-37FABE#pwd
flash:/log/
rfs7000-37FABE#```
3.1.5 change-passwd

Privileged Exec Mode Commands

Changes the password of a logged user. When this command is executed without any parameters, the password can be changed interactively.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
change-passwd \{<OLD-PASSWORD>\} <NEW-PASSWORD>
```

Parameters

- `change-passwd \{<OLD-PASSWORD>\} <NEW-PASSWORD>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;OLD-PASSWORD&gt;</code></td>
<td>Optional. Specify the password to be changed.</td>
</tr>
<tr>
<td><code>&lt;NEW-PASSWORD&gt;</code></td>
<td>Specify the new password. Note: The password can also be changed interactively. To do so, press [Enter] after the command.</td>
</tr>
</tbody>
</table>

Usage Guidelines

A password must be from 1 - 64 characters.

Examples

```
rfs7000-37FABE#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory{write memory} to be persistent.
rfs7000-37FABE#write memory
OK
rfs7000-37FABE#
```
### 3.1.6 clear

**Privileged Exec Mode Commands**

Clears parameters, cache entries, table entries, and other entries. The clear command is available for specific commands only. The information cleared using this command varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

---

**NOTE:** When using the `clear` command, refer to the interface details provided in **Chapter 7, PROFILES, section interface.**

#### Syntax

```plaintext
clear [arp-cache|bonjour|cdp|counters|crypto|event-history|firewall|gre|ip|ipv6|l2tpv3-stats|license|lldp|logging|mac-address-table|mint|role|rtls|smart-cache|spanning-tree|traffic-shape|vrrp]
clear arp-cache {on <DEVICE-NAME>}
clear bonjour cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear counters [all|ap|bridge|interface|radio|router|thread|wireless-client]
clear counters [all|bridge|router|thread]
clear counters [ap|wireless-client] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
clear counters interface [<INTERFACE-NAME>|all|ge <1-X>|me1|port-channel <1-X>|pppoe1|vlan <1-4094>|wan1|vmif <1-X>|xge <1-4>]
clear counters radio {<MAC/HOSTNAME>|on}
clear crypto [ike|ipsec]
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
clear crypto ipsec sa {on <DEVICE-NAME>}
clear event-history

clear firewall dhcp snoop-table|dos stats|flows [ipv4|ipv6]|neighbors snoop-table
    {on <DEVICE-NAME>}
clear firewall stats {on <DEVICE-NAME>}
clear ip [bgp|dhcp|ospf]
clear ip bgp [<IP>|all|external|process]
clear ip bgp [<IP>|all|external] {in|on|out|soft}
clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}
clear ip bgp [<IP>|all|external] {out} {on <DEVICE-NAME>}
clear ip bgp [<IP>|all|external] {soft {in|out}} {on <DEVICE-NAME>}
clear ip bgp process {on <DEVICE-NAME>}
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}
clear ipv6 neighbor-cache {on <DEVICE-NAME>}
```
clear l2tpv3-stats tunnel <L2TPV3-TUNNEL-NAME> {session <SESSION-NAME>} 
  {on <DEVICE-NAME>}

clear license [borrowed|lent]
clear license borrowed {on <DEVICE-NAME>}
clear license lent to <DEVICE-NAME> {on <DEVICE-NAME>}

clear logging {on <DEVICE-NAME>}

clear mac-address-table {address|interface|vlan} {on <DEVICE-NAME>}

clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table interface [{IF-NAME}|ge <1-X]|port-channel <1-X>
  tel <1-4> <1-1>|up <1-X>|vmif <1-X|xge <1-4>} {on <DEVICE-NAME>}

clear mint mlcp history {on <DEVICE-NAME>}

clear role ldap-stats {on <DEVICE-NAME>}

clear rtls [aeroscout|ekahau]
clear rtls [aeroscout|ekahau] {<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}|
  on <DEVICE-OR-DOMAIN-NAME>}

clear spanning-tree detected-protocols {interface|on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface [{INTERFACE-NAME}|ge <1-x]|me1|
  port-channel <1-x>|pppoel|vlan <1-4094>|wwan1|vmif <1-X|xge <1-4>}
  {on <DEVICE-NAME>}

clear traffic-shape statistics {class <1-4>} {(on <DEVICE-NAME>)}

clear vrrp [error-stats|stats] {on <DEVICE-NAME>}

The following clear command is specific to the NX45XX, NX65XX, and NX9XXX series service platforms:
clear smart-cache storage [all|url-regex <WORD>] {on <DEVICE-NAME>}

clear logging analytics {on <DEVICE-NAME>}

Parameters
  • clear arp-cache {on <DEVICE-NAME>}

  **arp-cache**
  Clears Address Resolution Protocol (ARP) cache entries on a device. This protocol
  matches layer 3 IP addresses to layer 2 MAC addresses.

  on <DEVICE-NAME>
  Optional. Clears ARP cache entries on a specified device
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service
    platform.

  • clear bonjour cache {on <DEVICE-NAME>}

  **bonjour cache**
  Clears all Bonjour cached statistics. Once cleared, the system has to re-discover
  available Bonjour services.

  on <DEVICE-NAME>
  Optional. Clears all Bonjour cached statistics on a specified device
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service
    platform.

  • clear [cdp|lldp] neighbors {on <DEVICE-NAME>}

  **cdp**
  Clears Cisco Discovery Protocol (CDP) table entries

  **lldp**
  Clears Link Layer Discovery Protocol (LLDP) neighbor table entries
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbors</td>
<td>Clears CDP or LLDP neighbor table entries based on the option selected in the preceding step</td>
</tr>
</tbody>
</table>
| on `<DEVICE-NAME>` | Optional. Clears CDP or LLDP neighbor table entries on a specified device  
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |

- **clear counters [all|bridge|router|thread]**
  
  **counters [all|bridge|router|thread]** | Clears counters on a system  
  - all – Clears all counters irrespective of the interface type  
  - bridge – Clears bridge counters  
  - router – Clears router counters  
  - thread – Clears per-thread counters |

- **clear counters [ap|wireless-client] `{<MAC}>` `{on <DEVICE-OR-DOMAIN-NAME>}`**
  
  `<MAC>` | The following keyword is common to the ‘ap’ and ‘wireless-client’ parameters:  
  - `<MAC>` – Optional. Clears counters of the AP/wireless client identified by the `<MAC>` keyword. Specify the MAC address of the AP or wireless client.  
  **Note:** The system clears all AP or wireless client counters, if no MAC address is specified. |

- **clear counters interface [INTERFACE-NAME]|all|ge <1-X>|me1|port-channel <1-X>|pppoel|vlan <1-4094>|wwan1|vmif <1-X>|xge <1-4>**
  
  `INTERFACE-NAME` | Clears interface counters for a specified interface  
  - `INTERFACE-NAME` – Clears a specified interface counters. Specify the interface name.  
  - all – Clears all interface counters  
  - `ge <1-X>` – Clears GigabitEthernet interface counters. Specify the GigabitEthernet interface index from 1 - X.  
  **Note:** The number of Ethernet interfaces supported varies for different device types. For example, the NX45XX and NX65XX support 24 GE interfaces. Where as, RFS4000 supports 5 GE interfaces.  
  - `me1` – Clears FastEthernet interface counters  
  - `port-channel <1-X>` – Clears port-channel interface counters. Specify the port channel interface index from 1 - X.  
  **Note:** The number of port-channel interfaces supported varies for different device types. For example, the NX45XX and NX65XX support 13 port-channels. Where as, RFS4000 supports 3 port-channels.  
  Contd..
### clear counters radio

- **clear counters radio** `{<MAC/HOSTNAME> <1-X>} {(on <DEVICE-OR-DOMAIN-NAME>)}`

  **counters radio**
  - Clears wireless radio counters

  **<MAC/HOSTNAME> <1-X>**
  - Clears counters of a radio identified by the `<MAC/HOSTNAME>` keyword.
    - `<MAC/HOSTNAME>` – Optional. Specify the hostname or MAC address.
      Optionally, append the interface number to form radio ID in the form of AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX
    - `<1-X>` – Optional. Specify the radio index (if not specified as part of the radio ID).
      The maximum number of radio antennas supported varies with the access point type.
      **Note:** If no MAC address or radio index is specified, the system clears all radio counters.

  **on <DEVICE-OR-DOMAIN-NAME>**
  - The following keyword is recursive and is applicable to the `<MAC>` parameter:
    - `<DEVICE-OR-DOMAIN-NAME>` – Optional. Clears AP/wireless-client counters on a specified device or RF Domain
      - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.
      **Note:** If no MAC address is specified, the system clears all AP or wireless client counters on the specified AP, wireless controller, service platform, or RF Domain.

### clear crypto ike sa

- **clear crypto ike sa** `[<IP>|all] {on <DEVICE-NAME>}`

  **crypto**
  - Clears encryption module database

  **ike sa** `[<IP>|all]`
  - Clears *Internet Key Exchange* (IKE) *security associations* (SAs)
    - `<IP>` – Clears IKE SAs for a certain peer
    - `all` – Clears IKE SAs for all peers

  **on <DEVICE-NAME>**
  - Optional. Clears IKE SA entries, for a specified peer or all peers, on a specified device
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

### clear crypto ipsec sa

- **clear crypto ipsec sa** `{on <DEVICE-NAME>}`

  **crypto**
  - Clears encryption module database

  **ipsec sa** `{on <DEVICE-NAME>}`
  - Clears *Internet Protocol Security* (IPSec) database SAs
    - `<DEVICE-NAME>` – Optional. Clears IPSec SA entries on a specified device
      - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.
### clear event-history

<table>
<thead>
<tr>
<th>event-history</th>
<th>Clears event history cache entries</th>
</tr>
</thead>
</table>

### clear firewall [dhcp snoop-table|dos stats|flows [ipv4|ipv6]|neighbors snoop-table] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>firewall</th>
<th>Clears firewall event entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp snoop-table</td>
<td>Clears DHCP snoop table entries</td>
</tr>
<tr>
<td>dos stats</td>
<td>Clears denial of service statistics</td>
</tr>
<tr>
<td>flows [ipv4</td>
<td>ipv6]</td>
</tr>
<tr>
<td>neighbors snoop-table</td>
<td>Clears IPv6 neighbors snoop-table entries</td>
</tr>
</tbody>
</table>
| on <DEVICE-NAME>                 | The following keywords are common to the DHCP, DOS, and flows parameters:  
  - on <DEVICE-NAME> – Optional. Clears DHCP snoop table entries, denial of service statistics, or the established firewall sessions on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

### clear gre stats {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>gre stats</th>
<th>Clears GRE tunnel statistics</th>
</tr>
</thead>
</table>
| on <DEVICE-NAME>                 | Optional. GRE tunnel statistics on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

### clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}

| ip bgp [<IP>|all|external]         | Clears BGP routing table information based on the option selected  
  - <IP> – Clears the BGP peer identified by the <IP> keyword. Specify the BGP peer’s IP address.  
  - all – Clears Route Updates Received From All BGP Peers  
  - external – Clears route updates received from external BGP peers  
  Note: This command is applicable only to the RFS4000, RFS6000, NX45XX, NX65XX, NX9000, and NX9600 series service platforms.  
  Note: In case of a change in routing policy it is necessary to clear BGP routing table entries in order for the new policy to take effect. |
| in prefix-filter                  | Optional. Clears soft-reconfiguration inbound route updates  
  - prefix-filter – Optional. Clears the existing Outbound Route Filtering (ORF) prefix-list. |
| on <DEVICE-NAME>                 | Optional. Clears soft-reconfiguration inbound route updates on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP or service platform. |
### clear ip bgp `<IP>|all|external` `{out}` `{on <DEVICE-NAME>}`

**ip bgp`<IP>|all|external>`: Clears BGP routing table information based on the option selected
- `<IP>` – Clears the BGP peer identified by the `<IP>` keyword. Specify the BGP peer’s IP address.
- all – Clears route updates received from all BGP peers
- external – Clears route updates received from external BGP peers

**Note:** This command is applicable only to the RFS4000, RFS6000, NX45XX, NX65XX, and NX9000 series service platforms.

**Note:** In case of a change in routing policy it is necessary to clear BGP routing table entries in order for the new policy to take effect.

**out** Optional. Clears soft-reconfiguration outbound route updates. Optionally specify the device on which to execute this command.

**on `<DEVICE-NAME>`**

The following keyword is recursive and optional.
- on `<DEVICE-NAME>` – Optional. Clears BGP sessions on a specified device
- `<DEVICE-NAME>` – Specify the name of the AP or service platform.

### clear ip bgp `<IP>|all|external` `{soft in|out}` `{on <DEVICE-NAME>}`

**ip bgp `<IP>|all|external>`: Clears BGP routing table information based on the option selected
- `<IP>` – Clears the BGP peer identified by the `<IP>` keyword. Specify the BGP peer’s IP address.
- all – Clears route updates received from all BGP peers
- external – Clears route updates received from external BGP peers

**Note:** This command is applicable only to the RFS4000, RFS6000, NX45XX, NX65XX, and NX9000 series service platforms.

**Note:** In case of a change in routing policy it is necessary to clear BGP routing table entries in order for the new policy to take effect.

**soft `{in|out}`** Optional. Enables soft-reconfiguration of route updates for the specified IP address. This option allows routing tables to be reconfigured without clearing BGP sessions.
- in – Optional. Enables soft reconfiguration of inbound route updates
- out – Optional. Enables soft reconfiguration of outbound route updates

**Note:** Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy etc.) take effect only after on-going BGP sessions are cleared. The `clear > ip > bgp` command clears BGP sessions. To reduce loss of route updates during the process, use the ‘soft’ option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage.

**on `<DEVICE-NAME>`** Optional. Clears soft-reconfiguration inbound/outbound route updates on a specified device
- `<DEVICE-NAME>` – Specify the name of the AP or service platform.

### clear ip bgp process `{on `<DEVICE-NAME>`}`

**ip bgp process** Clears all BGP processes running

**Note:** This command is applicable only to the RFS4000, RFS6000, NX45XX, NX65XX, NX9000, NX9600 platforms.

**on `<DEVICE-NAME>`** Optional. Clears all BGP processes on a specified device
- `<DEVICE-NAME>` – Specify the name of the AP or service platform.
• clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Clears a Dynamic Host Configuration Protocol (DHCP) server’s IP address bindings entries</td>
</tr>
<tr>
<td>dhcp bindings</td>
<td>Clears DHCP server’s connections and address binding entries</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Clears specific address binding entries. Specify the IP address to clear binding entries.</td>
</tr>
<tr>
<td>all</td>
<td>Clears all address binding entries</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears a specified address binding or all address bindings on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

• clear ip ospf process {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf process</td>
<td>Clears already enabled open shortest path first (OSPF) process and restarts the process</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears OSPF process on a specified device</td>
</tr>
<tr>
<td></td>
<td>OSPF is a link-state interior gateway protocol (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet layer which makes routing decisions based solely on the destination IP address found in IP packets.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

• clear ipv6 neighbor-cache {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 neighbor-cache</td>
<td>Clears IPv6 neighbor cache entries</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears IPv6 neighbor cache entries on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

• clear l2tpv3-stats tunnel <L2TPV3-TUNNEL-NAME> {session <SESSION-NAME>} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2tpv3-stats</td>
<td>Clears L2TPv3 tunnel session statistics</td>
</tr>
<tr>
<td>tunnel</td>
<td>Clears all sessions associated with a specified L2TPv3 tunnel</td>
</tr>
<tr>
<td>&lt;L2TPV3-TUNNEL-NAME&gt;</td>
<td>• &lt;L2TPV3-TUNNEL-NAME&gt; – Specify the L2TPv3 tunnel name.</td>
</tr>
<tr>
<td>session</td>
<td>Optional. Clears a specified L2TPv3 tunnel session, identified by the &lt;SESSION-NAME&gt; keyword</td>
</tr>
<tr>
<td>&lt;SESSION-NAME&gt;</td>
<td>• &lt;SESSION-NAME&gt; – Specify the session name.</td>
</tr>
</tbody>
</table>
### clear license borrowed

The following parameter is recursive and optional:
- **on <DEVICE-NAME>** – Optional. Specifies the device running the L2TPv3 tunnel session.
- **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

**Note:** If no optional parameters are specified, the system clears all L2TPv3 tunnel session statistics.

```
• clear license borrowed {on <DEVICE-NAME>}
```

### license borrowed

Releases or revokes all licenses borrowed by a site controller.

- **on <DEVICE-NAME>** – Optional. Specifies the borrowing controller’s name.

**Note:** If no device name is specified, the system clears all borrowed licenses on the logged device.

```
license borrowed {on <DEVICE-NAME>}
```

### clear license lent

NOC controller releases or revokes all licenses loaned to a site controller.

- **on <DEVICE-NAME>** – Optional. Specifies the controller’s name.

**Note:** If no device name is specified, the system clears all loaned licenses on the logged device.

```
license lent to <DEVICE-NAME> {on <DEVICE-NAME>}
```

### clear mac-address-table

Clears the MAC address forwarding table.

- **address <MAC>** – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF
- **vlan <1-4094>** – Specify the VLAN ID from 1 - 4094

```
• clear mac-address-table {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}
```

### interface

Clears all MAC addresses for the selected interface. Use the options available to specify the interface.

```
• clear mac-address-table interface [<IF-NAME>|ge <1-X>|port-channel <1-X>|t1e1 <1-4> <1-1>|up <1-X>|vmif <1-X>|xge <1-4>] {on <DEVICE-NAME>}
```

- **<IF-NAME>** – Specify the layer 2 interface name.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ge &lt;1-X&gt;</code></td>
<td>Clears MAC address forwarding table for the specified GigabitEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-X&gt;</code> – Specify the GigabitEthernet interface index from 1 - X.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The number of Ethernet interfaces supported varies for different device types. For example the NX45XX and NX65XX support 24 GE interfaces. Where as, RFS4000 supports 5 GE interfaces.</td>
</tr>
<tr>
<td><code>port-channel &lt;1-X&gt;</code></td>
<td>Clears MAC address forwarding table for the specified port-channel interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-X&gt;</code> – Specify the port-channel interface index from 1 - X.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The number of port-channel interfaces supported varies for different device types. For example, the NX45XX and NX65XX support 13 port-channels. Where as, RFS4000 supports 3 port-channels.</td>
</tr>
<tr>
<td><code>t1e1 &lt;1-4&gt; &lt;1-1&gt;</code></td>
<td>Clears MAC address forwarding table for the specified T1E1L interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-4&gt;</code> – Specify the T1E1 interface index from 1 - 4. A maximum of 4 slots are available. Select the slot to clear the MAC address forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-1&gt;</code> – Specify the T1E1 port ID from 1 - 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The T1E1 interfaces are supported only on the NX45XX and NX65XX series service platforms.</td>
</tr>
<tr>
<td><code>up &lt;1-X&gt;</code></td>
<td>Clears MAC address forwarding table for the WAN Ethernet interface</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The number of WAN Ethernet interfaces supported varies for different devices. The RFS4000 and RFS6000 devices support 1 WAN Ethernet interface. The NX45XX supports 2 WAN Ethernet interfaces.</td>
</tr>
<tr>
<td><code>vmif &lt;1-X&gt;</code></td>
<td>Clears MAC address forwarding table for the VM interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-X&gt;</code> – Specify the VM interface index from 1 - X.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The VMIF interfaces are supported only on the NX45XX, NX65XX, NX9500, NX9510, NX9600 series service platforms. The number of supported VMIFs varies for different device types.</td>
</tr>
<tr>
<td><code>xge &lt;1-4&gt;</code></td>
<td>Clears MAC address forwarding table for the specified TenGigabitEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-4&gt;</code> – Specify the GigabitEthernet interface index from 1 - 4.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This interface is supported only on the NX9000 series service platforms.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- `clear mint mlcp history {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mint</code></td>
<td>Clears MiNT related information</td>
</tr>
<tr>
<td><code>mlcp history</code></td>
<td>Clears MiNT Link Creation Protocol (MLCP) client history</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Clears MLCP client history on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform</td>
</tr>
</tbody>
</table>

- `clear role ldap-stats {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>role ldap-stats</code></td>
<td>Clears role based Lightweight Directory Access Protocol (LDAP) server statistics</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Clears role based LDAP server statistics on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>
• clear rtls [aeroscout|ekahau] \{<MAC/DEVICE-NAME> \{on <DEVICE-OR-DOMAIN-NAME>\}|on <DEVICE-OR-DOMAIN-NAME>\}

<table>
<thead>
<tr>
<th>rtls</th>
<th>Clears Real Time Location Service (RTLS) statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>aeroscout</td>
<td>Clears RTLS Aeroscout statistics</td>
</tr>
<tr>
<td>ekahau</td>
<td>Clears RTLS Ekahau statistics</td>
</tr>
<tr>
<td>&lt;MAC/DEVICE-NAME&gt;</td>
<td>This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.</td>
</tr>
<tr>
<td></td>
<td>• &lt;MAC/DEVICE-NAME&gt; – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, or service platform. Specify the AP’s MAC address or hostname.</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

• clear spanning-tree detected-protocols \{on <DEVICE-NAME>\}

<table>
<thead>
<tr>
<th>spanning-tree detected-protocols</th>
<th>Clears spanning tree protocols on an interface, and also restarts protocol migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears spanning tree protocols on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Optional. Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

• clear spanning-tree detected-protocols \{interface \[<INTERFACE-NAME>|ge <1-X>|me1|port-channel <1-X>|pppoe1|vlan <1-4094>|wwan1|vmif <1-X>|xge <1-4>\]\{on <DEVICE-NAME>\}

<table>
<thead>
<tr>
<th>spanning-tree detected-protocols</th>
<th>Clears spanning tree protocols on an interface and restarts protocol migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface [&lt;INTERFACE-NAME&gt;</td>
<td>ge &lt;1-X&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;INTERFACE-NAME&gt; – Clears detected spanning tree entries on a specified interface. Specify the interface name.</td>
</tr>
<tr>
<td></td>
<td>• ge &lt;1-X&gt; – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - X</td>
</tr>
<tr>
<td>Note: The number of Ethernet interfaces supported varies for different device types. For example the NX45XX and NX65XX support 24 GE interfaces. Where as, RFS400 supports 5 GE interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• me1 – Clears FastEthernet interface spanning tree entries</td>
</tr>
<tr>
<td></td>
<td>• port-channel &lt;1- X&gt; – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - X.</td>
</tr>
<tr>
<td>Note: The number of port-channel interfaces supported varies for different device types. For example the NX45XX and NX65XX support 13 port-channels. Where as, RFS400 supports 3 port-channels.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pppoe1 – Clears detected spanning tree entries for PPPoE interface.</td>
</tr>
<tr>
<td></td>
<td>• vlan &lt;1-4094&gt; – Clears detected spanning tree entries for the selected VLAN interface. Select a SVI VLAN ID from 1 - 4094.</td>
</tr>
</tbody>
</table>
| Contd..                         | }
### clear traffic-shape statistics

Clears traffic shaping statistics

<table>
<thead>
<tr>
<th>class &lt;1-4&gt;</th>
<th>(on &lt;DEVICE-NAME&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Clears traffic shaping statistics for a specific traffic class</td>
<td></td>
</tr>
<tr>
<td>&lt;1-4&gt; – Specify the traffic class from 1 - 4.</td>
<td></td>
</tr>
<tr>
<td>Note: If the traffic class is not specified, the system clears all traffic shaping statistics.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>on &lt;DEVICE-NAME&gt;</th>
<th>Optional. Clears traffic protocol entries on a selected device</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

### vrrp

Clears Virtual Router Redundancy Protocol (VRRP) statistics for a device

<table>
<thead>
<tr>
<th>error-stats</th>
<th>(on &lt;DEVICE-NAME&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears global error statistics</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; – Optional. Clears VRRP global error statistics on a selected device</td>
<td></td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt; – Specify the name of the access point, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>stats</th>
<th>(on &lt;DEVICE-NAME&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears VRRP related statistics</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; – Optional. Clears VRRP related statistics on a selected device</td>
<td></td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

### smart-cache

Clears the smart-cache storage

Smart caching is a licensed service available on the NX45XX and NX65XX series service platforms. It allows the temporary storage of frequently accessed Web content (Web pages, graphics, audio and video files etc.) on network infrastructure devices. When this content is requested, it is retrieved from a local content cache and not from the origin server. For more information on enabling content caching, see smart-cache-policy.
### PRIVILEGED EXEC MODE COMMANDS

| storage [all|regex <WORD>] | Clears stored content based on the parameters passed  
|---------------------------|-----------------------------------------------------|
|                           | - all – Clears all cached content  
|                           | - regex <WORD> – Clears only those URLs matching the specified expression  
|                           |  - <WORD> – Provide the URL in the following format: e.g. \\.xxx\/\+.\.(flv|mp4)  

| on <DEVICE-NAME> | Optional. Clears stored content on a specified device  
|-------------------|-----------------------------------------------------|
|                   | - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform  

### Examples

```
rfs4000-229D58#clear crypto ike sa all
rfs4000-229D58#show crypto ike sa
---------------------------------------------------------------------------------------
IDX PEER VERSION ENCR ALGO HASH ALGO DH GROUP IKE STATE
---------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------
Total IKE SAs: 0
rfs4000-229D58#
```

```
rfs7000-37FABE#clear spanning-tree detected-protocols interface port-channel 1
rfs7000-37FABE#clear ip dhcp bindings 172.16.10.9
rfs7000-37FABE#clear cdp neighbors
rfs4000-229D58#clear spanning-tree detected-protocols interface ge 1
rfs4000-229D58#clear lldp neighbors
rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2015-03-18 09:01:07 IST' by 'admin'
2015-03-18 09:01:00     rfs4000-229D58  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-03-17 11:08:39     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
'admin' with privilege 'superuser' from '192.168.100.220'
2015-03-17 10:38:37     rfs4000-229D58  SYSTEM     CONFIG_REVISION      Configuration
revision updated to 4 from 3
2015-03-17 10:38:37     rfs4000-229D58  SYSTEM     CONFIG_COMMIT        Configuration
commit by user 'admin' (mapsh) from '192.168.100.220'
2015-03-17 10:34:26     rfs4000-229D58  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
--More--
rfs4000-229D58#
rfs4000-229D58#show event-history
rfs4000-229D58#clear event-history
EVENT HISTORY REPORT
Generated on '2015-03-18 09:02:32 IST' by 'admin'
rfs4000-229D58#```
nx4500-5CFA2B#show mac-address-table

<table>
<thead>
<tr>
<th>BRIDGE</th>
<th>VLAN</th>
<th>PORT</th>
<th>MAC</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-15-70-38-06-49</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-0F-8F-19-BA-4C</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-5C-FA-8E</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-15-70-81-74-2D</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-23-68-0F-43-D8</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-A0-F8-68-D5-64</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-6C-88-09</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>5C-0E-8B-18-10-91</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-02-B3-28-D1-55</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>3C-CE-73-F4-47-83</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-15-70-37-FD-F2</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-58-72-58</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-71-17-28</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-23-68-13-9B-34</td>
<td>forward</td>
</tr>
</tbody>
</table>

Total number of MACs displayed: **14**

nx4500-5CFA2B#

nx4500-5CFA2B#clear mac-address-table vlan 1

nx4500-5CFA2B#show mac-address-table

<table>
<thead>
<tr>
<th>BRIDGE</th>
<th>VLAN</th>
<th>PORT</th>
<th>MAC</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-15-70-38-06-49</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-0F-8F-19-BA-4C</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-5C-FA-8E</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-15-70-81-74-2D</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-23-68-0F-43-D8</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-A0-F8-68-D5-64</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-6C-88-09</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>B4-C7-99-71-17-28</td>
<td>forward</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>up1</td>
<td>00-23-68-13-9B-34</td>
<td>forward</td>
</tr>
</tbody>
</table>

Total number of MACs displayed: **9**

nx4500-5CFA2B#
3.1.7 clock

Sets a device’s system clock. By default all WiNG devices are shipped with the time zone and time format set to UTC and 24-hour clock respectively. If a device’s clock is set without resetting the time zone, the time is displayed relative to the Universal Time Coordinated (UTC) – Greenwich Time. For example, San Jose is approximately 7 or 8 hours (depending on the time of the year) behind the UTC time. If the time at Greenwich, UK is 15:00:00 UTC, at San Jose it will display as 8:00:00 or 7:00:00 UTC. To display time in the local time zone format, in the device’s configuration mode, use the timezone command to reset the time zone. You can also reset the time zone at the RF Domain level. When configured as RF Domain setting, it applies to all devices within the domain. Configuring the local time zone prior to setting the clock is recommended. For more information on configuring RF Domain time zone, see timezone.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}

Parameters

- clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}

| clock set | Sets a device’s system clock |
| <HH:MM:SS> | Sets the current time (in military format hours, minutes and seconds)  
**Note:** By default the WiNG software displays time in the 24-hour clock format. This setting cannot be changed. |
| <1-31> | Sets the numerical day of the month |
| <MONTH> | Sets the month of the year from Jan - Dec |
| <1993-2035> | Sets a valid four digit year from 1993 - 2035 |

on <DEVICE-NAME> Optional. Sets the clock on a specified device

- <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

The following commands set the time zone and clock for the logged device:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#timezone America/Los_Angeles
```

```
nx9500-6C8809#clock set 10:13:00 24 Mar 2015
```

```
nx9500-6C8809#show clock
2015-03-24 10:13:07 PDT
```

Note, if the clock is set without resetting the time zone, the time displays as UTC time as shown in the following example:

```
nx4500-5CFA2B#show clock
2015-09-08 06:19:34 UTC
```

```
nx4500-5CFA2B#```
### 3.1.8 cluster

- **Privileged Exec Mode Commands**

  Initiates the cluster context. The cluster context provides centralized management to configure all cluster members from any one member.

  Commands executed under this context are executed on all members of the cluster.

  Supported in the following platforms:
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
cluster start-election
```

**Parameters**

- `cluster start-election`

**Examples**

```
rfs7000-37FABE#cluster start-election
rfs7000-37FABE#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>create-cluster</code></td>
<td>Creates a new cluster on a specified device</td>
</tr>
<tr>
<td><code>join-cluster</code></td>
<td>Adds a controller, as cluster member, to an existing cluster of devices</td>
</tr>
</tbody>
</table>
3.1.9 configure

Privileged Exec Mode Commands

Enters the configuration mode. Use this command to enter the current device’s configuration mode, or enable configuration from the terminal.

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
configure {self|terminal}

Parameters
• configure {self|terminal}

<table>
<thead>
<tr>
<th>self</th>
<th>Optional. Enables the current device’s configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal</td>
<td>Optional. Enables configuration from the terminal</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE#configure self
Enter configuration commands, one per line. End with CNTL/Z.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs7000-37FABE(config)#
3.1.10 connect

Privileged Exec Mode Commands

Begins a console connection to a remote device using the remote device’s MiNT ID or name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]

Parameters
- connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]

Examples
rfs7000-6DCD4B#show mint lsp-db
6 LSPs in LSP-db of 19.6D.CD.4B:
LSP 19.58.72.58 at level 1, hostname "ap5142-587258", 5 adjacencies, seqnum 748149
LSP 19.5C.FA.2B at level 1, hostname "nx4500-5CFA2B", 5 adjacencies, seqnum 337443
LSP 19.5C.FA.8E at level 1, hostname "nx4500-5CFA8E", 5 adjacencies, seqnum 333443
LSP 19.6C.88.09 at level 1, hostname "nx9500-6C8809", 5 adjacencies, seqnum 333247
LSP 19.6D.CD.4B at level 1, hostname "rfs7000-6DCD4B", 5 adjacencies, seqnum 152431
LSP 19.71.17.28 at level 1, hostname "ap8132-711728", 5 adjacencies, seqnum 363523
rfs7000-6DCD4B#connect mint-id 19.6C.88.09

Entering character mode
Escape character is '\'.

NX9500 release 5.8.1.0-020D
nx9500-6C8809 login:admin
Password:
nx9500-6C8809>
3.11 copy

Privileged Exec Mode Commands

Copies a file (config, log, txt... etc) from any location to the access point, wireless controller, or service platform and vice-versa.

**NOTE:** Copying a new config file to an existing running-config file merges it with the existing running-config file on the wireless controller. Both the existing running-config and the new config file are applied as the current running-config.

Copying a new config file to a start-up config file replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]
```

**Parameters**

- `<SOURCE-FILE>` Specify the source file to copy.
- `<SOURCE-URL>` Specify the source file’s location (URL).
- `<DESTINATION-FILE>` Specify the destination file to copy to.
- `<DESTINATION-URL>` Specify the destination file’s location (URL).

**Examples**

Transferring file snmpd.log to remote TFTP server.
```
rfs7000-37FABE#copy flash:/log/snmpd.log tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote TFTP server into switch running-config.
```
rfs7000-37FABE#copy tftp://157.235.208.105:/running-config running-config
```
3.1.12 cpe

Privileged Exec Mode Commands

Enables a WiNG controller to perform certain operations on Customer Premises Equipment (CPEs) through an adopted T5 controller.

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5’s management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE’s physical wallplate connection and phone jack.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

cpe [boot|led|reload|upgrade]

cpe boot system cpe [<1-24>|all] [primary|secondary] {on <T5-DEVICE-NAME>}

cpe [led|reload|upgrade <IMAGE-LOCATION>] cpe [<1-24>|all] {on <T5-DEVICE-NAME>}

Parameters

- cpe boot system cpe [<1-24>|all] [primary|secondary] {on <T5-DEVICE-NAME>}

<table>
<thead>
<tr>
<th>cpe boot system</th>
<th>Changes the image used by a CPE to boot. When reloading, the CPE uses the specified image.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpe [&lt;1-24&gt;</td>
<td>all]</td>
</tr>
<tr>
<td>[primary</td>
<td>secondary]</td>
</tr>
<tr>
<td>on &lt;T5-DEVICE-NAME&gt;</td>
<td>Optional. Performs this operation on a specified T5 device</td>
</tr>
</tbody>
</table>

| cpe [led|reload|upgrade <IMAGE-LOCATION>] | Performs the following operations on CPEs |
|------------------------------------------|-----------------------------------------|
| led – Enables flashing of LEDs |
| reload – Reloads the device |
| upgrade <IMAGE-LOCATION> – Upgrades the device |
| <IMAGE-LOCATION> – Specify the location of the firmware image. Both IPv4 and IPv6 addresses are supported. |

Contd..
Use one of the following options to provide the location:
IPv4 URLs: tftp://<hostname/IP>[:port]/path/file
ftp://<user>:@<hostname/IP>[:port]/path/file
sftp://<user>:@<hostname/IP>[:port]/path/file
http://<hostname/IP>[:port]/path/file
cf:/path/file
usb<n>:/path/file
IPv6 URLs: tftp://<hostname/[IPv6]>[:port]/path/file
ftp://<user>:@<hostname/[IPv6]>[:port]/path/file
sftp://<user>:@<hostname/[IPv6]>[:port]/path/file

**Note:** After specifying the operation to perform, identify the device(s).

| cpe [<1-24>|all] | Identifies the CPE(s) on which the operation is performed |
|------------------|----------------------------------------------------------|
| • <1-24> – Configures the CPE’s ID from 1 - 24 |
| • all – Configures all CPEs |

<table>
<thead>
<tr>
<th>on &lt;T5-DEVICE-NAME&gt;</th>
<th>Optional. Performs this operation on a specified T5 device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;T5-DEVICE-NAME&gt; – Specify the T5 device’s hostname.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**
rfs7000-37FABE#cpe led cpe all on t5-ED5C2C
Updated T5 CPE led state
rfs7000-37FABE#
### 3.1.13 create-cluster

 privileget Exec Mode Commands

Creates a new device cluster, with the specified name, and assigns it an IP address and routing level.

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```bash
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

#### Parameters

- `create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name &lt;CLUSTER-NAME&gt;</td>
<td>Configures the cluster name</td>
</tr>
<tr>
<td>ip &lt;IP&gt;</td>
<td>Specifies the device’s IP address used for cluster creation</td>
</tr>
<tr>
<td>level [1</td>
<td>2]</td>
</tr>
</tbody>
</table>

#### Examples

```bash
rfs4000-229D58# create-cluster name TechPubsLAN ip 192.168.13.8 level 2
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs4000-229D58#
```

```bash
rfs4000-229D58# show cluster configuration
```

Cluster Configuration Information
- Name: TechPubsLAN
- Configured Mode: Active
- Master Priority: 128
- Force configured state: Disabled
- Force configured state delay: 5 minutes
- Handle STP: Disabled

```bash
rfs4000-229D58#
```
rfs4000-229D58#show context
!
! Configuration of RFS4000 version 5.8.1.0-021D
!
!
version 2.3
!
sage-type request option 60 exact ascii "dhcpcd 4.0.15"
.................................................................
!!
rfs4000 00-23-68-22-9D-58
use profile default-rfs4000
use rf-domain default
hostname rfs4000-229D58
license AP DEFAULT-6AP-LICENSE
license ADSEC DEFAULT-ADV-SEC-LICENSE
mint mlcp vlan
mint mlcp ip
wep-shared-key-auth
ip default-gateway 192.168.13.2
interface ge1
  switchport mode access
  switchport access vlan 1
interface vlan1
  ip address 192.168.13.9/24
  ip address 192.168.0.1/24 secondary
  ip dhcp client request options all
interface vlan2
  ip address 1.2.3.5/24
cluster name TechPubsLAN
cluster mode active
cluster member ip 192.168.13.8 level 2
logging on
logging console debugging
logging buffered warnings
!
end
rfs4000-229D58#

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cluster</strong></td>
</tr>
<tr>
<td><strong>join-cluster</strong></td>
</tr>
</tbody>
</table>
3.14 crypto

Privileged Exec Mode Commands

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by CAs and contain user or device specific information, such as name, public key, IP address, serial number, company name etc. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate Certificate Signing Request (CSR).

This command also enables trustpoint configuration. Trustpoints contain the CA's identity and configuration parameters.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

crypto [key|pki]

crypto key [export|generate|import|zeroize]

crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> 
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background|on|passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> 
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}

crypto pki [authenticate|export|generate|import|zeroize]

crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL> {background}
{(on <DEVICE-NAME>)}
crypto pki export [request|trustpoint]

crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME> 
[autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> 
autogen-subject-name <(EXPORT-TO-URL),email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>}
crypto pki export request [generate-rsa-key|short |generate-rsa-key|use-rsa-key] | 
use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> <(EXPORT-TO-URL),email <SEND-TO-EMAIL>, 
fqdn <FQDN>,ip-address <IP>}
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> 
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}

crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key| 
use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key| 
use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name <(email <SEND-TO-EMAIL>, 
fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] 
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> <(email <SEND-TO-EMAIL>,fqdn <FQDN>, 
ip-address <IP>,on <DEVICE-NAME>)}
### crypto pki import [certificate|crl|trustpoint]
### crypto pki import [certificate | crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL> 
{background} {on <DEVICE-NAME>}
### crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> 
{background | passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}
### crypto pki zeroize trustpoint <TRUSTPOINT-NAME> 
{del-key} {on <DEVICE-NAME>}

#### Parameters
- **crypto key export rsa** <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> 
  {background | passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}
- **crypto key generate rsa** <RSA-KEYPAIR-NAME> [2048|4096] 
  {on <DEVICE-NAME>}
- **crypto key import rsa** <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> 
  {background | passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>key</th>
<th>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</th>
</tr>
</thead>
</table>
| export rsa <RSA-KEYPAIR-NAME> | Exports an existing RSA Keypair to a specified destination  
  • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.  
  <EXPORT-TO-URL> Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported.  
  After specifying the destination address (where the RSA keypair is exported), configure one of the following parameters: background or passphrase. |
| background | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on. |
| passphrase <KEY-PASSPHRASE> background | Optional. Encrypts RSA Keypair before exporting  
  • <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA keypair.  
  • background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on. |
| on <DEVICE-NAME> | The following parameter is recursive and common to all of the above parameters:  
  • on <DEVICE-NAME> – Optional. Performs export operation on a specified device  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- **crypto key generate rsa** <RSA-KEYPAIR-NAME> [2048|4096] 
  {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>key</th>
<th>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</th>
</tr>
</thead>
</table>
| generate rsa <RSA-KEYPAIR-NAME> [2048|4096] | Generates a new RSA Keypair  
  • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.  
  • [2048|4096] – Sets the size of the RSA key in bits. The options are 2048 bits and 4096 bits. The default size is 2048 bits.  
  After specifying the key size, optionally specify the device (access point or controller) to generate the key on. |
| on <DEVICE-NAME> | Optional. Generates the new RSA Keypair on a specified device  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- **crypto key import rsa** <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> 
  {background | passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>key</th>
<th>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>import rsa</strong></td>
<td>Imports a RSA Keypair from a specified source</td>
</tr>
<tr>
<td><code>&lt;RSA-KEYPAIR-NAME&gt;</code></td>
<td>- <code>&lt;RSA-KEYPAIR-NAME&gt;</code> – Specify the RSA Keypair name.</td>
</tr>
<tr>
<td><code>&lt;IMPORT-FROM-URL&gt;</code></td>
<td>Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported. After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase.</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.</td>
</tr>
<tr>
<td>passphrase</td>
<td>Optional. Decrypts the RSA Keypair after importing</td>
</tr>
<tr>
<td><code>&lt;KEY-PASSPHRASE&gt;</code></td>
<td>- <code>&lt;KEY-PASSPHRASE&gt;</code> – Specify the passphrase to decrypt the RSA keypair.</td>
</tr>
<tr>
<td>background</td>
<td>- background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on.</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-NAME&gt;</code></td>
<td>The following parameter is recursive and common to the ‘background’ and ‘passphrase’ keywords:</td>
</tr>
<tr>
<td></td>
<td>- on <code>&lt;DEVICE-NAME&gt;</code> – Optional. Performs import operation on a specific device</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- `crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>key</strong></td>
<td>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</td>
</tr>
<tr>
<td>zeroize rsa</td>
<td>Deletes a specified RSA Keypair</td>
</tr>
<tr>
<td><code>&lt;RSA-KEYPAIR-NAME&gt;</code></td>
<td>- <code>&lt;RSA-KEYPAIR-NAME&gt;</code> – Specify the RSA Keypair name.</td>
</tr>
<tr>
<td>force</td>
<td>Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion.</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-NAME&gt;</code></td>
<td>The following parameter is recursive and optional:</td>
</tr>
<tr>
<td></td>
<td>- on <code>&lt;DEVICE-NAME&gt;</code> – Optional. Deletes all certificates associated with the RSA Keypair on a specified device</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- `crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background} {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>pki</strong></td>
<td>Enables Private Key Infrastructure (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated Certificate Authority (CA) certificates.</td>
</tr>
<tr>
<td>authenticate</td>
<td>Authenticated a trustpoint and imports the corresponding CA certificate</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>- <code>&lt;TRUSTPOINT-NAME&gt;</code> – Specify the trustpoint name.</td>
</tr>
<tr>
<td><code>&lt;URL&gt;</code></td>
<td>Specify CA's location. Both IPv4 and IPv6 address formats are supported.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The CA certificate is imported from the specified location.</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the authentication on.</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| on <DEVICE-NAME> | The following parameter is recursive and optional:  
  • on <DEVICE-NAME> – Optional. Performs authentication on a specified device  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)

| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| export request | Exports CSR to the CA for digital identity certificate. The CSR contains applicant’s details and RSA Keypair’s public key. |
| [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair  
  • generate-rsa-key – Generates a new RSA Keypair for digital authentication  
  • use-rsa-key – Uses an existing RSA Keypair for digital authentication  
  • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |

- autogen-subject-name | Auto generates subject name from configuration parameters. The subject name identifies the certificate. |
| <EXPORT-TO-URL> | Specify the CA's location. Both IPv4 and IPv6 address formats are supported.  
  Note: The CSR is exported to the specified location. |
| email <SEND-TO-EMAIL> | Exports CSR to a specified e-mail address  
  • <SEND-TO-EMAIL> – Specify the CA’s e-mail address. |
| fqdn <FQDN> | Exports CSR to a specified Fully Qualified Domain Name (FQDN)  
  • <FQDN> – Specify the CA’s FQDN. |
| ip-address <IP> | Exports CSR to a specified device or system  
  • <IP> – Specify the CA’s IP address. |

- crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)

<p>| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. |
| export request | Exports CSR to the CA for a digital identity certificate. The CSR contains applicant’s details and RSA Keypair’s public key. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki</td>
<td>Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.</td>
</tr>
<tr>
<td>export trustpoint</td>
<td>Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key. Specify the trustpoint name (should be authenticated).</td>
</tr>
<tr>
<td>export trustpoint &lt;TRUSTPOINT-NAME&gt;</td>
<td>Specify the destination address. Both IPv4 and IPv6 address formats are supported. The trustpoint is exported to the address specified here.</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on.</td>
</tr>
</tbody>
</table>

### Trustpoint Export Command

```plaintext
[generate-rsa-key] short [generate-rsa-key|use-rsa-key]] use-rsa-key] <RSA-KEYPAIR-NAME>
```

Generates a new RSA Keypair or uses an existing RSA Keypair
- `generate-rsa-key` – Generates a new RSA Keypair for digital authentication
- `short generate-rsa-key|use-rsa-key` – Generates and exports a shorter version of the CSR
- `generate-rsa-key` – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it.
- `use-rsa-key` – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name.
- `use-rsa-key` – Uses an existing RSA Keypair for digital authentication
- `<RSA-KEYPAIR-NAME>` – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.

### Subject Name Configuration

```plaintext
subject-name <COMMON-NAME>
```

Configures a subject name, defined by the `<COMMON-NAME>` keyword, to identify the certificate
- `<COMMON-NAME>` – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).

### Country Configuration

```plaintext
<COUNTRY>
```

Sets the deployment country code (2 character ISO code)

### State Configuration

```plaintext
<STATE>
```

Sets the state name (2 to 64 characters in length)

### City Configuration

```plaintext
<CITY>
```

Sets the city name (2 to 64 characters in length)

### Organization Configuration

```plaintext
<ORGANIZATION>
```

Sets the organization name (2 to 64 characters in length)

### Organization Unit Configuration

```plaintext
<ORGANIZATION-UNIT>
```

Sets the organization unit (2 to 64 characters in length)

### Export-to-URL Configuration

```plaintext
<EXPORT-TO-URL>
```

Specify the CA's location. Both IPv4 and IPv6 address formats are supported. The CSR is exported to the specified location.

### Email Configuration

```plaintext
del fcredit email <SEND-TO-EMAIL>
```

Exports CSR to a specified e-mail address
- `<SEND-TO-EMAIL>` – Specify the CA’s e-mail address.

### FQDN Configuration

```plaintext
fqdn <FQDN>
```

Exports CSR to a specified FQDN
- `<FQDN>` – Specify the CA’s FQDN.

### IP Address Configuration

```plaintext
ip-address <IP>
```

Exports CSR to a specified device or system
- `<IP>` – Specify the CA’s IP address.

---

```
• crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background|passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}
```

---

### Other Commands

- `pki` Enables PKI management.
- `export trustpoint` Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key.
- `<EXPORT-TO-URL>` Specify the destination address. Both IPv4 and IPv6 address formats are supported. The trustpoint is exported to the address specified here.
| passphrase | Optional. Encrypts the key with a passphrase before exporting  
| <KEY-PASSPHRASE> | • <KEY-PASSPHRASE> – Specify the passphrase to encrypt the trustpoint.  
| background | • background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.  
| on <DEVICE-NAME> | The following parameter is recursive and common to the ‘background’ and ‘passphrase’ keywords:  
| <DEVICE-NAME> | • on <DEVICE-NAME> – Optional. Performs export operation on a specified device  
| <DEVICE-NAME> | • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.  

**crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name {<email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>}}**

| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.  
| generate | Generates a certificate and a trustpoint  
| self-signed | Generates a self-signed certificate and a trustpoint  
| <TRUSTPOINT-NAME> | • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.  
| [generate-rsa-key|use-rsa-key] | Generates a new RSA Keypair, or uses an existing RSA Keypair  
| <RSA-KEYPAIR-NAME> | • generate-rsa-key – Generates a new RSA Keypair for digital authentication  
| | • use-rsa-key – Uses an existing RSA Keypair for digital authentication  
| | • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.  
| autogen-subject-name | Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate.  
| email <SEND-TO-EMAIL> | Optional. Exports the self-signed certificate to a specified e-mail address  
| <SEND-TO-EMAIL> | • <SEND-TO-EMAIL> – Specify the e-mail address.  
| fqdn <FQDN> | Optional. Exports the self-signed certificate to a specified FQDN  
| <FQDN> | • <FQDN> – Specify the FQDN.  
| ip-address <IP> | Optional. Exports the self-signed certificate to a specified device or system  
| <IP> | • <IP> – Specify the device’s IP address.  
| on <DEVICE-NAME> | Optional. Exports the self-signed certificate on a specified device  
| <DEVICE-NAME> | • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.  

**crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> {<email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>}}**

| pki | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.  
| generate self-signed | Generates a self-signed certificate and a trustpoint  
| <TRUSTPOINT-NAME> | • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.  

---

**pki**

Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.

**generate self-signed**

Generates a self-signed certificate and a trustpoint

**<TRUSTPOINT-NAME>**

• <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[generate-rsa-key]</td>
<td>Generates a new RSA Keypair, or uses an existing RSA Keypair</td>
</tr>
<tr>
<td>use-rsa-key</td>
<td>• generate-rsa-key – Generates a new RSA Keypair for digital authentication</td>
</tr>
<tr>
<td>[RSA-KEYPAIR-NAME]</td>
<td>• use-rsa-key – Uses an existing RSA Keypair for digital authentication</td>
</tr>
<tr>
<td></td>
<td>• [RSA-KEYPAIR-NAME] – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.</td>
</tr>
<tr>
<td>subject-name</td>
<td>Configures a subject name, defined by the &lt;COMMON-NAME&gt; keyword, to identify the certificate</td>
</tr>
<tr>
<td>[COMMON-NAME]</td>
<td>• &lt;COMMON-NAME&gt; – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length.</td>
</tr>
<tr>
<td>&lt;COUNTRY&gt;</td>
<td>Sets the deployment country code (2 character ISO code)</td>
</tr>
<tr>
<td>&lt;STATE&gt;</td>
<td>Sets the state name (2 to 64 characters in length)</td>
</tr>
<tr>
<td>&lt;CITY&gt;</td>
<td>Sets the city name (2 to 64 characters in length)</td>
</tr>
<tr>
<td>&lt;ORGANIZATION&gt;</td>
<td>Sets the organization name (2 to 64 characters in length)</td>
</tr>
<tr>
<td>&lt;ORGANIZATION-UNIT&gt;</td>
<td>Sets the organization unit (2 to 64 characters in length)</td>
</tr>
<tr>
<td>email</td>
<td>Optional. Exports the self-signed certificate to a specified e-mail address</td>
</tr>
<tr>
<td>[SEND-TO-EMAIL]</td>
<td>• [SEND-TO-EMAIL] – Specify the e-mail address.</td>
</tr>
<tr>
<td>fqdn</td>
<td>Optional. Exports the self-signed certificate to a specified FQDN</td>
</tr>
<tr>
<td>[FQDN]</td>
<td>• [FQDN] – Specify the FQDN.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Optional. Exports the self-signed certificate to a specified device or system</td>
</tr>
<tr>
<td>[IP]</td>
<td>• [IP] – Specify the device’s IP address.</td>
</tr>
</tbody>
</table>

**crypto pki import**

<table>
<thead>
<tr>
<th>[certificate</th>
<th>crl] &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt; {background} {(on &lt;DEVICE-NAME&gt;)}</th>
</tr>
</thead>
<tbody>
<tr>
<td>pki</td>
<td>Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.</td>
</tr>
<tr>
<td>import</td>
<td>Imports certificates, Certificate Revocation List (CRL), or a trustpoint to the selected device</td>
</tr>
<tr>
<td>[certificate</td>
<td>crl] &lt;TRUSTPOINT-NAME&gt;</td>
</tr>
<tr>
<td></td>
<td>• certificate – Imports signed server certificate</td>
</tr>
<tr>
<td></td>
<td>• crl – Imports CRL</td>
</tr>
<tr>
<td></td>
<td>• [TRUSTPOINT-NAME] – Specify the trustpoint name (should be authenticated).</td>
</tr>
<tr>
<td>&lt;IMPORT-FROM-URL&gt;</td>
<td>Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported. The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here.</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following parameter is recursive and optional:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Performs import operation on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>
**crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background|passphrase <KEY-PASSPHRASE> background} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>pki</th>
<th>Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>import</td>
<td>Imports certificates, CRL, or a trustpoint to the selected device</td>
</tr>
<tr>
<td>trustpoint &lt;TRUSTPOINT-NAME&gt;</td>
<td>Imports a trustpoint and its associated CA certificate, server certificate, and private key</td>
</tr>
<tr>
<td></td>
<td>• &lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be authenticated).</td>
</tr>
<tr>
<td>&lt;IMPORT-FROM-URL&gt;</td>
<td>Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported.</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on.</td>
</tr>
<tr>
<td>passphrase</td>
<td>Optional. Decrypts trustpoint with a passphrase after importing</td>
</tr>
<tr>
<td>&lt;KEY-PASSPHRASE&gt; background</td>
<td>• &lt;KEY-PASSPHRASE&gt; – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on.</td>
</tr>
<tr>
<td></td>
<td>• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following parameter is recursive and optional:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Performs import operation on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>pki</th>
<th>Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>zeroize trustpoint &lt;TRUSTPOINT-NAME&gt;</td>
<td>Deletes a trustpoint and its associated CA certificate, server certificate, and private key</td>
</tr>
<tr>
<td></td>
<td>• &lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be authenticated).</td>
</tr>
<tr>
<td>del-key</td>
<td>Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following parameter is recursive and optional:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Deletes the trustpoint on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:

- IPv4 URLs:
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:@<hostname|IP>[:port]/path/file
  - sftp://<user>:@<hostname|IP>[:port]/path/file
  - http://<hostname|IP>[:port]/path/file
  - cf:/path/file
usb<n>:/path/file

- IPv6 URLs:
  - tftp://<hostname|[IPv6]>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file
  - sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file

**Examples**

```
rfs7000-37FABE#crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs7000-37FABE#
```

```
rfs7000-37FABE#crypto key import rsa test123 url passphrase word background
RSA key import operation is started in background
rfs7000-37FABE#
```

```
rfs7000-37FABE#crypto pki generate self-signed word generate-rsa-key word autogen-
subject-name fqdn word
Successfully generated self-signed certificate
rfs7000-37FABE#
```

```
rfs7000-37FABE#crypto pki zeroize trustpoint word del-key
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-trustpoint
rfs7000-37FABE#
```

```
rfs7000-37FABE#crypto pki authenticate word url background
Import of CA certificate started in background
rfs7000-37FABE#
```

```
rfs7000-37FABE#crypto pki import trustpoint word url passphrase word
Import operation started in background
rfs7000-37FABE#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes server certificates, trustpoints and their associated certificates</td>
</tr>
</tbody>
</table>
### 3.1.15 crypto-cmp-cert-update

**Privileged Exec Mode Commands**

Triggers a Certificate Management Protocol (CMP) certificate update on a specified device or devices.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
crypto-cmp-cert-update <TRUSTPOINT-NAME>{on <DEVICE-NAME>}
```

**Parameters**

- `crypto-cmp-cert-update <TRUSTPOINT-NAME>{on <DEVICE-NAME>}`  
  - Triggers a CMP certificate update on a specified device or devices:  
    - `<TRUSTPOINT-NAME>` – Specify the target trustpoint name. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. Use the crypto-cmp-policy context to configure the trustpoint.  
    - `<DEVICE-NAME>` – Optional. Triggers a CMP certificate update and response on a specified device or devices. Specify the name of the AP, wireless controller, or service platform. Multiple devices can be provided as a comma separated list.

**Examples**

```
rfs4000-229D58#crypto-cmp-cert-update test on B4-C7-99-71-17-28  
CMP Cert update success  
rfs4000-229D58#
```
3.1.16 database

▶ Privileged Exec Mode Commands

Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight). Vacuuming a database refers to the process of finding and reclaiming space left over from previous DELETE statements. Supported in the following platforms:
  • Service Platforms — NX9000, NX9500, NX9510, NX9600

Syntax

database [drop|repair]
database drop [all|captive-portal|nsight]
database repair {on <DEVICE-NAME>}

Parameters
  • database drop [all|captive-portal|nsight]
  • database repair {on <DEVICE-NAME>}

| database drop [all|captive-portal|nsight] | Drops (deletes) all or a specified database
|------------------------------------------|---------------------------------|
|                                          | • all – Drops all databases, captive portal and NSight.
|                                          | • captive-portal – Drops captive-portal database only
|                                          | • nsight – Drops NSight database only

| database repair {on <DEVICE-NAME>} | Enables automatic repairing of all databases
|------------------------------------|--------------------------------------------------------|
|                                    | • on <DEVICE-NAME> – Optional. Specifies the name of the access point, wireless controller, or service platform hosting the database. When specified, databases on the specified device are periodically checked through to identify and remove obsolete data documents.
|                                    | • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
|                                    | If no device is specified, the system repairs all databases.

Examples

nx9500-6C8809#database repair on nx9500-6C8809
nx9500-6C8809#

Related Commands

<table>
<thead>
<tr>
<th>database-backup</th>
<th>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server</th>
</tr>
</thead>
<tbody>
<tr>
<td>database-restore</td>
<td>Restores a previously exported database [captive-portal and/or NSight]</td>
</tr>
</tbody>
</table>
### 3.1.17 database-backup

- **Privileged Exec Mode Commands**

  Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server.

  Supported in the following platforms:
  - Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

```
database-backup database [captive-portal|nsight] <URL>
```

**Parameters**

- `database-backup database [captive-portal|nsight] <URL>`

| database-backup database [captive-portal|nsight] | Backs up captive portal and/or NSight database to a specified location and file. Select the database to backup:
| | - captive-portal – Backs up captive portal database
| | - nsight – Backs up NSight database
| <URL> | Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:
| | - ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
| | - sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz

**Examples**

```
nx9500-6C8809#database-backup database nsight ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

**Related Commands**

<table>
<thead>
<tr>
<th><strong>database</strong></th>
<th>Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>database-restore</strong></td>
<td>Restores a previously exported (backed up) database [captive-portal and/or NSight]</td>
</tr>
</tbody>
</table>
3.1.18 database-restore

Privileged Exec Mode Commands

Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored from the backed-up location to the original database.

Supported in the following platforms:
  • Service Platforms — NX9000, NX9500, NX9510, NX9600

Syntax

database-restore database [captive-portal|nsight] <URL>

Parameters

- database-restore database [captive-portal|nsight] <URL>

| database-restore database [captive-portal|nsight] | Restores previously exported (backed up) captive-portal and/or NSight database. Specify the database type:
| | • captive-portal – Restores captive portal database
| | • nsight – Restores NSight database
| | After specifying the database type, configure the destination location and file name from where the files are restored.

| <URL> | Configures the destination location. The database is restored from the specified location. Specify the location URL in one of the following formats:
| | ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
| | sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz

Examples

nx9500-6C8809#database-restore database nsight
ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz

Related Commands

- database  Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)
- database-backup  Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server
3.1.19 delete

Privileged Exec Mode Commands

Deletes a specified file from the device's file system

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

del [force <FILE> | recursive <FILE> | <FILE>]

Parameters

- force [force <FILE> | recursive <FILE> | <FILE>]
- recursive <FILE> Performs a recursive delete
- <FILE> Specifies the file name
  * Deletes the file specified by the <FILE> parameter

Examples

rfs7000-37FABE#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

rfs7000-37FABE#delete /force flash:/tmp.txt
rfs7000-37FABE#

rfs7000-37FABE#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core
[y/n]? y
Delete
flash:/backup//fileMgmt_350_18212X.core_bk
[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz
[y/n]? n
rfs7000-37FABE#
3.1.20 device-upgrade

Privileged Exec Mode Commands

Enables firmware upgrade on an adopted device or a set of adopted devices (access points, wireless controllers, and service platforms)

This command simplifies device upgradation within a hierarchically managed (HM) network. For more information on HM networks, see device-upgrade.

NOTE: A NOC controller’s capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:

- NOC controller – RFS7000, NX9000, NX95XX (NX9500 and NX9510), NX9600
- Site controller – RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, or NX95XX

Within a HM network, the devices deployed as site controllers depends on the NOC controller device type. For more information on the adoption capabilities of various NOC controller devices, see Usage Guidelines (NOC controller adoption matrix).

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

device-upgrade [<MAC/HOSTNAME>|all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap82xx|rf34000|rf56000|rf67000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|vx9000|cancel-upgrade|load-image|rf-domain]

device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>}/
    upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}

device-upgrade all {force|no-reboot|reboot-time <TIME>}/upgrade-time <TIME> {no-reboot|
    reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf34000|rf56000|rf67000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|vx9000|all} {force|no-reboot|reboot-time <TIME>}/upgrade-time <TIME> {no-reboot|
    reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf34000|rf56000|rf67000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|vx9000|on rf-domain
    [RF-DOMAIN-NAME]|all]]

device-upgrade load-image [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf34000|rf56000|rf67000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|vx9000] [FILE-URL] on
    DEVICE-OR-DOMAIN-NAME]

device-upgrade rf-domain [<RF-DOMAIN-NAME]|all|containing <WORD>|filter location
    <WORD> [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf34000|rf56000|rf67000|nx45xx|nx5500|
    nx65xx|nx75xx|nx9000|nx9600|vx9000] {<MAC/HOSTNAME)|force|no-reboot|
    from-controller|reboot-time <TIME>}/staggered-reboot|upgrade-time <TIME>}


### Privileged Exec Mode Commands

#### Parameters

- **device-upgrade** `<MAC/HOSTNAME>` \{`no-reboot`|`reboot-time` `<TIME>`|`upgrade-time` `<TIME>`\} \{`no-reboot`|`reboot-time` `<TIME>`\}

  - Upgrades firmware on the device identified by the `<MAC/HOSTNAME>` keyword.
  - `<MAC/HOSTNAME>` – Specify the device’s MAC address or hostname.

- **device-upgrade** `all` \{`force`|`no-reboot`|`reboot-time` `<TIME>`|`upgrade-time` `<TIME>`\} \{`no-reboot`|`reboot-time` `<TIME>`\}

  - Upgrades firmware on all devices.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAC/HOSTNAME&gt;</code></td>
<td>Specifies the device's MAC address or hostname.</td>
</tr>
<tr>
<td>no-reboot</td>
<td>Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted).</td>
</tr>
<tr>
<td>reboot-time <code>&lt;TIME&gt;</code></td>
<td>Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>upgrade-time <code>&lt;TIME&gt;</code></td>
<td>Optional. Schedules an automatic device firmware upgrade on all devices on a specified day and time. Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>all</td>
<td>Upgrades firmware on all devices.</td>
</tr>
<tr>
<td>force</td>
<td>Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.</td>
</tr>
<tr>
<td>no-reboot</td>
<td>Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted).</td>
</tr>
<tr>
<td>reboot-time <code>&lt;TIME&gt;</code></td>
<td>Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>upgrade-time <code>&lt;TIME&gt;</code></td>
<td>Optional. Schedules an automatic device firmware upgrade on all devices on a specified day and time. Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>staggered-reboot</td>
<td>This keyword is recursive and common to all of the above.</td>
</tr>
</tbody>
</table>

#### Staggered Reboot

- Optional. Enables staggered device reboot (one at a time), without network impact.
device-upgrade <DEVICE-TYPE> all

Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000.

After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.

force

Optional. Select this option to force upgrade on selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.

no-reboot

Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted).

reboot-time <TIME>

Optional. Schedules an automatic reboot after a successful upgrade:

- <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

upgrade-time <TIME> {no-reboot|reboot-time <TIME>}

Optional. Schedules an automatic firmware upgrade on all devices of the specified type, on a specified day and time:

- <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade:
  - no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
  - reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

staggered-reboot

This keyword is recursive and common to all of the above:

- Optional. Enables staggered device reboot (one at a time), without network impact.

cancel-upgrade [<MAC/HOSTNAME>|all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|vx9000 on rf-domain [<RF-DOMAIN-NAME>|all]]

Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades:

- Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames.
- Cancels upgrade on all devices within the network.
- Cancels upgrade on all devices of a specific type. Specify the device type.
- Cancels upgrade on specific device or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name.

cancel-upgrade [<MAC/HOSTNAME>|all]

Cancels a scheduled firmware upgrade on a specified device or on all devices

- <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device’s MAC address or hostname.
- all – Cancels scheduled upgrade on all devices
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel-upgrade</td>
<td>Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000.</td>
</tr>
</tbody>
</table>
| cancel-upgrade on rf-domain   | Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains  
• `<RF-DOMAIN-NAME>` – Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name.  
• `all` – Cancels scheduled device upgrade on all devices across all RF Domains |
| load-image                   | Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image.  
• `<DEVICE-TYPE>` – Specify the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000. After specifying the device type, provide the location of the required device firmware image. |
| `<IMAGE-URL>`                | Specify the device’s firmware image location in one of the following formats:  
IPv4 URLs:  
- `tftp://<hostname/IP>[:port]/path/file`  
- `ftp://<user>:<passwd>@<hostname/IP>[:port]/path/file`  
- `sftp://<user>:<passwd>@<hostname/IP>[:port]/path/file`  
- `http://<hostname/IP>[:port]/path/file`  
- `cf:/path/file`  
- `usb<n>:/path/file`  
IPv6 URLs:  
- `tftp://<hostname[IPv6]>[:port]/path/file`  
- `ftp://<user>:<passwd>@<hostname[IPv6]>[:port]/path/file`  
- `sftp://<user>:<passwd>@<hostname[IPv6]>[:port]/path/file`  
- `cf:/path/file`  
- `usb<n>:/path/file`  
| on `<DEVICE-OR-DOMAIN-NAME>` | Optional. Specifies the name of a device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded.  
• `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>] [all|ap621|ap622|ap650|ap651|ap652|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45XX|nx5500|nx55XX|nx75xx|nx9000|nx9600|vx9000] {(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>|staggered-reboot|upgrade-time <TIME>)}

| rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>]| Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager.  
  • <RF-DOMAIN-NAME> – Upgrades devices in the RF Domain identified by the <RF-DOMAIN-NAME> keyword.  
  • <RF-DOMAIN-NAME> – Specify the RF Domain name.  
  • all – Upgrades devices across all RF Domains  
  • containing <WORD> – Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the <WORD> keyword are filtered. Devices on the filtered RF Domains are upgraded.  
  • filter location <WORD> – Filters devices by their location. All devices with location matching the <WORD> keyword are upgraded.

| <DEVICE-TYPE> | After specifying the RF Domain, select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX55XX, NX75XX, NX9000, NX9600, VX9000. After specifying the RF Domain and the device type, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.

| <MAC/HOSTNAME> | Optional. Use this option to identify specific devices for upgradation. Specify the device's MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.  
  **Note:** If no MAC address or hostname is specified, all devices of the type selected are upgraded.

| force | Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.

| from-controller | Optional. Upgrades a device through the adopting device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.

| no-reboot {staggered-reboot} | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)

| reboot-time <TIME> {staggered-reboot} | Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

| staggered-reboot | This keyword is common to all of the above.  
  Optional. Enables staggered reboot (one at a time), without network impact.
upgrade-time <TIME> {no-reboot|reboot-time <TIME>}

Optional. Schedules an automatic firmware upgrade
• <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.
  After a scheduled upgrade, the following actions can be performed:
  • no-reboot – Optional. Disables automatic reboot after a successful upgrade
    (the device must be manually restarted)
  • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful
    upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

Usage Guidelines (NOC controller adoption matrix)
The following table displays NOC controllers and the corresponding site-level controllers supported by each:

<table>
<thead>
<tr>
<th>Site Controllers supported by each NOC controller</th>
<th>RFS7000</th>
<th>NX9000</th>
<th>NX95XX (NX9500 &amp; NX9510)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RFS6000</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RFS7000</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX45XX</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX65XX</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX7500</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX9000</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>NX95XX</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

Examples
rfs7000-6DCD4B#device-upgrade rfs6000-81742D

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-CD-4B</td>
<td>Success</td>
<td>Queued 1 devices to upgrade</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B#

rfs7000-6DCD4B#show device-upgrade history

<table>
<thead>
<tr>
<th>Device</th>
<th>RESULT</th>
<th>TIME</th>
<th>RETRIES</th>
<th>UPGRADED-BY</th>
<th>LAST-UPDATE-ERROR</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2014-11-17 02:42:27</td>
<td>0</td>
<td>rfs7000-6DCD4B</td>
<td>-</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2015-01-16 01:19:36</td>
<td>0</td>
<td>rfs7000-6DCD4B</td>
<td>-</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>failed</td>
<td>2014-09-28 23:25:45</td>
<td>3</td>
<td>rfs7000-6DCD4B</td>
<td>Reboot failed</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2014-07-11 00:02:47</td>
<td>0</td>
<td>rfs7000-6DCD4B</td>
<td>-</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2014-11-30 21:54:11</td>
<td>0</td>
<td>rfs7000-6DCD4B</td>
<td>-</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2015-01-05 05:35:53</td>
<td>0</td>
<td>rfs7000-6DCD4B</td>
<td>-</td>
</tr>
</tbody>
</table>
--More--
rfs7000-6DCD4B#
rfs7000-6DCD4B#show device-upgrade versions

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>DEVICE-TYPE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap621</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap622</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap650</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap6511</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap6521</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap6522</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap6532</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap6562</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap71xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap7502</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap7532</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap7562</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap81xx</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>ap82xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>rfs4000</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>rfs6000</td>
<td>5.8.1.0-027D</td>
</tr>
<tr>
<td>rfs7000-6DCD4B</td>
<td>rfs7000</td>
<td>none</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B#
3.1.21 diff

Privileged Exec Mode Commands

Displays the differences between two files on a device’s file system or a particular URL.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

diff [FILE] [URL]

Parameters
- diff [FILE] [URL]
- <FILE> The first <FILE> is the source file for the diff command. The second <FILE> is used for comparison.
- <URL> The first <URL> is the source file’s URL. The second <URL> is the second file’s URL.

Examples

rfs4000-229D58#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
+! Configuration of RFS4000 version 5.8.1.0-021D
+! @@ -107,14 +108,11 @@
+ controller-managed
+ rfs4000 00-23-68-22-9D-58
- radio-count 0
+ use profile default-rfs4000
+ use rf-domain default
+ hostname rfs4000-229D58
+ license AP DEFAULT-6AP-LICENSE
+ license ADSEC DEFAULT-ADV-SEC-LICENSE
- model-number RFS-4010-00010-WR
- adoption-site B4-C7-99-6C-88-09
+ mint mlcp vlan
+ mint mlcp ip
+ ip default-gateway 192.168.13.2
@@ -140,8 +138,6 @@
+ hostname nx4500-5CFA2B
+ license AP DEFAULT-12AP-LICENSE
+ license ADSEC DEFAULT-ADV-SEC-LICENSE
- model-number NX-4500-0000-00-WR
- adoption-site B4-C7-99-6C-88-09
+ ip default-gateway 192.168.13.2
+ interface vlan1
+ ip address 192.168.13.12/24

rfs4000-229D58#
3.1.22 dir

Privileged Exec Mode Commands

Lists files on a device’s file system

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dir {/all|/recursive|<DIR>|all-filesystems}

Parameters

- dir {/all|/recursive|<DIR>|all-filesystems}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/all</td>
<td>Optional. Lists all files</td>
</tr>
<tr>
<td>/recursive</td>
<td>Optional. Lists files recursively</td>
</tr>
<tr>
<td>&lt;DIR&gt;</td>
<td>Optional. Lists files in the named file path</td>
</tr>
<tr>
<td>all-filesystems</td>
<td>Optional. Lists files on all file systems</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809# dir flash: /
Directory of flash: /

```
drwx Tue Mar 17 07:01:39 2015 crashinfo
drwx Thu May 16 09:29:10 2013 upgrade
drwx Thu Apr 16 08:48:48 2015 log
drwx Fri Apr 17 09:31:59 2015 archived_logs
drwx Thu May 16 09:29:10 2013 cache
drwx Thu Feb 19 08:53:45 2015 floorplans
-rw- 29708288 Wed Mar 18 06:32:13 2015 in.tar
drwx Mon Sep 15 03:40:02 2014 hotspot
```

nx9500-6C8809#

nx9500-6C8809# dir all-filesystems
Directory of flash: /

```
drwx Tue Mar 17 07:01:39 2015 crashinfo
drwx Thu May 16 09:29:10 2013 upgrade
drwx Thu Apr 16 08:48:48 2015 log
drwx Fri Apr 17 09:32:57 2015 archived_logs
drwx Thu May 16 09:29:10 2013 cache
drwx Thu Feb 19 08:53:45 2015 floorplans
-rw- 29708288 Wed Mar 18 06:32:13 2015 in.tar
drwx Mon Sep 15 03:40:02 2014 hotspot
```

Directory of nvram: /

```
lwx 40 Thu Oct 3 03:59:47 2013 default-client-identity-config
-rw- 43052 Thu Apr 16 08:48:46 2015 startup-config
-rw- 189 Thu Apr 16 08:48:52 2015 licenses
-rw- 174 Thu Apr 16 08:48:53 2015 app_dict.pkl
lwx 26 Mon Jan 20 06:19:20 2014 bonjour_services
-rw- 870 Thu Apr 16 08:49:53 2015 app_stats_dict.pkl
```

nx9500-6C8809#
3.1.23 **disable**

*Privileged Exec Mode Commands*

Turns off (disables) the privileged mode command set. This command returns to the User Executable mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

disable

**Parameters**

None

**Examples**

rfs7000-37FABE#disable
rfs7000-37FABE>
3.1.24 edit

Privileged Exec Mode Commands

Edits a text file on the device’s file system

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
edit <FILE>

Parameters
- edit <FILE>

Examples
rfs4000-229D58#edit startup-config
GNU nano 1.2.4                File: startup-config

! Configuration of RFS4000 version 5.8.1.0-021D
!
! version 2.3
!
client-identity Android-2-2
dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
client-identity Android-2-3
dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
dhcp 1 message-type request option-codes exact hexstring 353d32393c37
dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
!
client-identity Android-2-3-x
[ line 1/808 (0%), col 1/2 (50%), char 0/22694 (0%) ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Txt ^T To Spell
3.1.25  enable

Privileged Exec Mode Commands

Turns on (enables) the privileged mode command set. This command does not do anything in the Privilege Executable mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

enable

Parameters

None

Examples

rfs7000-37FABE#enable
rfs7000-37FABE#
## 3.1.26 erase

### Privileged Exec Mode Commands

Erases a device's (wireless controller, access point, and service platform) file system. Erases the content of the specified storage device. Also erases the startup configuration to restore the device to its default.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>erase startup-config</code></td>
<td>Erases the startup configuration file.</td>
</tr>
<tr>
<td><code>erase startup-config</code></td>
<td>Parameters</td>
</tr>
<tr>
<td><code>&lt;HOSTNAME/MAC&gt;</code></td>
<td>Optional. Erases the startup configuration file on the device</td>
</tr>
<tr>
<td><code>&lt;DOMAIN-NAME&gt;</code></td>
<td>identified by the <code>&lt;HOSTNAME/MAC&gt;</code> keyword. Specify the device</td>
</tr>
<tr>
<td><code>&lt;SUB-STRING&gt;</code></td>
<td>device's hostname or MAC address.</td>
</tr>
</tbody>
</table>

### Parameters

- **flash:** Erases everything in the device's flash: file
- **nvram:** Erases everything in the device's nvram: file
- **startup-config:** Erases the device's startup configuration file. The startup configuration file is used to configure the device when it reboots.
- **usb1:** Erases everything in the device's usb1: file
  - **Note:** The number of USB ports displayed varies for different device types. For example, an NX95XX has two USB ports, while an NX45XX has four USB ports.
- **usb2:** Erases everything in the device's usb2: file
- **usb3:** Erases everything in the device's usb3: file
- **usb4:** Erases everything in the device's usb4: file
- **<HOSTNAME/MAC>/on <DOMAIN-NAME>** {containing `<SUB-STRING>`/exclude-controllers|exclude-rf-domain-manager|filter `<DEVICE-TYPE>`}
Examples

nx4500-5CFA2B#erase ?
  flash:          Erase everything in flash:
  nvram:          Erase everything in nvram:
  startup-config Reset configuration to factory default
  usb1:           Erase everything in usb1:
  usb2:           Erase everything in usb2:
  usb3:           Erase everything in usb3:
  usb4:           Erase everything in usb4:

nx4500-5CFA2B#

In the following example shows the startup configuration file being erased on a device having hostname ‘rfs6000-81701D’:

rfs7000-6DCD4B#erase startup-config rfs6000-81701D

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-81-70-1D</td>
<td>Success</td>
<td>None</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B#
Privileged Exec Mode Commands

Enables EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP-related configurations.

The copy keyword provides multiple copy options. It allows you to upload or download code images or configuration files between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

Syntax

ex3500 [adopted|boot|copy|delete|ip]

ex3500 adopted upgrade <URL> on <EX3500-DEVICE-NAME>

ex3500 boot system <1-1> (config|opcode) <FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 copy [file|ftp|running-config|tftp|unit]

ex3500 copy [file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME]

ex3500 copy [ftp|tftp] [add-to-running-config|file|https-certificate|public-key|running-config|startup-config]


ex3500 copy [ftp|tftp] [running-config|startup-config] <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>


ex3500 copy unit file <1-1> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>

ex3500 delete [file|public-key]

ex3500 delete file [name <FILE-NAME>|unit <1-1> name <FILE-NAME>]

ex3500 delete public-key <USER-NAME> [dsa|rsa] on <EX3500-DEVICE-NAME>

ex3500 ip ssh [crypto|save]

ex3500 ip ssh crypto host-key generates [dsa|rsa] on <EX3500-DEVICE-NAME>
### PRIVILEGED EXEC MODE COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex3500 ip ssh crypto zeroize [dsa</td>
<td>rsa] on &lt;EX3500-DEVICE-NAME&gt;</td>
</tr>
<tr>
<td>ex3500 ip ssh save host-key on &lt;EX3500-DEVICE-NAME&gt;</td>
<td>Copies a specified file (this is the source configuration file)</td>
</tr>
<tr>
<td>- <code>ex3500 adopted upgrade &lt;URL&gt; on &lt;EX3500-DEVICE-NAME&gt;</code></td>
<td>Copies a specified file (this is the source configuration file)</td>
</tr>
<tr>
<td>- `ex3500 boot system &lt;1-1&gt; (config</td>
<td>opcode) &lt;FILE-NAME&gt; on &lt;EX3500-DEVICE-NAME&gt;`</td>
</tr>
<tr>
<td>- <code>ex3500 copy file &lt;SOURCE-FILE-NAME&gt; &lt;DEST-FILE-NAME&gt; on &lt;EX3500-DEVICE-NAME&gt;</code></td>
<td>Copies the file to a specified EX3500 switch. <strong>Note:</strong> As of now only one (1) EX3500 unit can be managed through a NOC controller.</td>
</tr>
</tbody>
</table>
**ex3500 copy [ftp|tftp] add-to-running-config** `<FTP/TFTP-SERVER-IP> <USER-NAME> <PASS-WORD> <SOURCE-FILE-NAME>` on `<EX3500-DEVICE-NAME>`

Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key etc. This command also allows you to add a remote system's running configuration to the current system configuration.

**add-to-running-config**

Adds a remote system’s running configuration to the current system.

- `<FTP/TFTP-SERVER-IP>` – Specify the FTP or TFTP server’s IP address in the A.B.C.D format.
- `<USER-NAME>` – If using a FTP server, specify the FTP server’s user name (should be an authorized user)
- `<PASS-WORD>` – Specify the password applicable for the above specified FTP server user name.

- `<SOURCE-FILE-NAME>` – Specify the source file's name

Copies the file to a specified EX3500 switch

- `<EX3500-DEVICE-NAME>` – Specify the EX3500 switch’s hostname. The specified source file is copied to specified destination file on the EX3500 identified here.


Copies to a specified file system

- `<FTP/TFTP-SERVER-IP>` – Specify the FTP or TFTP server’s IP address in the A.B.C.D format.
- `<USER-NAME>` – If using a FTP server, specify the FTP server’s user name (should be an authorized user)
- `<PASS-WORD>` – Specify the password applicable for the above specified FTP server user name.

- `[1|2]` – Select the file type from 1 - 2.
  - 1 – Copies the EX3500 configuration file.
  - 2 – Copies the opcode, which is the runtime code. The opcode is like an operating system that enables the WiNG software to communicate with the EX3500 device.
- `<SOURCE-FILE-NAME>` – Specify the source file’s name.
- `<DEST-FILE-NAME>` – Specify the destination file’s name.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FTP/TFTP-SERVER-IP&gt; &lt;USER-NAME&gt; &lt;PASSWORD&gt;</td>
<td>Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server.</td>
</tr>
<tr>
<td>&lt;SOURCE-CERT-FILE-NAME&gt; &lt;SOURCE-PVT-KEY-FILE-NAME&gt; &lt;PVT-PASS-WORD&gt;</td>
<td>After identifying the FTP or TFTP server, specify the following:</td>
</tr>
<tr>
<td>on &lt;EX3500-DEVICE-NAME&gt;</td>
<td>Copies the file to a specified EX3500 device</td>
</tr>
<tr>
<td>&lt;FTP/TFTP-SERVER-IP&gt; &lt;USER-NAME&gt; &lt;PASSWORD&gt;</td>
<td>Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server.</td>
</tr>
</tbody>
</table>

- **FTP/TFTP-SERVER-IP**: Specify the FTP or TFTP server's IP address in the A.B.C.D format.
- **USER-NAME**: If using a FTP server, specify the FTP server's user name (should be an authorized user).
- **PASSWORD**: Specify the password applicable for the above specified FTP server user name.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**ex3500 copy [ftp</td>
<td>tftp] [running-config</td>
</tr>
<tr>
<td>**ex3500 copy ftp</td>
<td>tftp**</td>
</tr>
</tbody>
</table>
| **[running-config|startup-config]** | Copies the running or startup configuration file to one of the following destinations: file system, FTP server, or TFTP server
The running configuration file can be copied to the startup configuration file and vice versa. |
| **<FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD>** | If copying to a FTP/TFTP server, configure the following parameters:
- **<FTP/TFTP-SERVER-IP>** – Specify the FTP or TFTP server’s IP address in the A.B.C.D format.
- **<USER-NAME>** – If using a FTP server, specify the FTP server’s user name (should be an authorized user)
- **<PASSWORD>** – Specify the password applicable for the above specified FTP server user name. |
| **<DEST-FILE-NAME>** | Configures the destination file name. The running or startup configuration file is copied to the specified destination file.
- **<DEST-FILE-NAME>** – Specify the destination file name. You can also copy the running configuration file to the startup configuration file and vice versa. |
| **on <EX3500-DEVICE-NAME>** | Copies the running or startup configuration file on to a specified EX3500 device
- **<EX3500-DEVICE-NAME>** – Specify the EX3500 device’s hostname. |
| **ex3500 copy unit file <1-1> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>** | Copies from a EX3500 switch
- **<1-1> [1|2]** – Specify the unit number from 1 - 1.
- **<SOURCE-FILE-NAME>** – Specify the source file name. You can copy the running configuration file to the startup configuration file and vice versa. |

**[1|2] <SOURCE-PUB-KEY-FILE-NAME> <USER-NAME>**

After identifying the FTP or TFTP server, specify the following:
- **[1|2]** – Configures the SSH public key type as RS or DSA
  - **1** – Configures the public key type as RSA
  - **2** – Configures the public key type as DSA
- **<SOURCE-PUB-KEY-FILE-NAME>** – Specifies the source public key file name
- **<USER-NAME>** – Specifies the public key’s user name.

**on <EX3500-DEVICE-NAME>**

Copies the public key to a specified EX3500 device
- **<EX3500-DEVICE-NAME>** – Specify the EX3500 device’s hostname.

**<SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> <PASSWORD>**

If copying to a FTP/TFTP server, configure the following parameters:
- **<FTP/TFTP-SERVER-IP>** – Specify the FTP or TFTP server’s IP address in the A.B.C.D format.
- **<USER-NAME>** – If using a FTP server, specify the FTP server’s user name (should be an authorized user)
- **<PASSWORD>** – Specify the password applicable for the above specified FTP server user name.

**<DEST-FILE-NAME>**

Configures the destination file name. The running or startup configuration file is copied to the specified destination file.
- **<DEST-FILE-NAME>** – Specify the destination file name. You can also copy the running configuration file to the startup configuration file and vice versa.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ex3500 delete file</code></td>
<td>Deletes a file or image on a specified EX3500 device</td>
<td><code>&lt;DEST-FILE-NAME&gt;</code> - Configures the destination file name. The running or startup configuration file is copied to the specified file.</td>
</tr>
<tr>
<td><code>ex3500 delete file</code></td>
<td>Deletes a file or image on a specified EX3500 device</td>
<td><code>&lt;FILE-NAME&gt;</code> - Specifies the file to delete. The specified file is deleted.</td>
</tr>
<tr>
<td><code>ex3500 delete</code></td>
<td>Copies the running or startup configuration file on to a specified EX3500 device</td>
<td><code>&lt;1-1&gt;</code> - Select the unit from 1 - 1. &lt;br&gt; <code>&lt;FILE-NAME&gt;</code> - Specify the file name.</td>
</tr>
<tr>
<td><code>ex3500 delete public-key</code></td>
<td>Deletes a specified user’s public key</td>
<td><code>&lt;USER-NAME&gt;</code> - Specify the SSH user’s name.</td>
</tr>
<tr>
<td><code>ex3500 ip ssh crypto host-key generates</code></td>
<td>Generates the host-key pair (public and private). This host key is used by the SSH server to negotiate a session key and encryption method with the client trying to connect to it.</td>
<td><code>&lt;EX3500-DEVICE-NAME&gt;</code> - Specify the EX3500 device’s hostname.</td>
</tr>
<tr>
<td><code>ex3500 ip ssh zeroize</code></td>
<td>Removes the host-key (DSA and RSA) from the volatile memory (i.e. RAM)</td>
<td><code>&lt;EX3500-DEVICE-NAME&gt;</code> - Specify the EX3500 device’s hostname.</td>
</tr>
</tbody>
</table>
on <EX3500-DEVICE-NAME> Executes the command on a specified EX3500 device
  • <EX3500-DEVICE-NAME> – Specify the EX3500 device’s hostname.

• ex3500 ip ssh save host-key on <EX3500-DEVICE-NAME>

ex3500 ip ssh save host-key Saves the host-key (DSA and RSA) to the flash memory

on <EX3500-DEVICE-NAME> Executes the command on a specified EX3500 device
  • <EX3500-DEVICE-NAME> – Specify the EX3500 device’s hostname.

Usage Guidelines
When using the ex3500 command and its parameters, keep in mind the following:

• Destination file names should not:
  • Contain slashes (\ or /).
  • Exceed 32 characters for files on the switch, or 127 characters for files on the server
  • The FTP server’s default user name is set as “anonymous”.
  • The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. Follow instructions provided in the release notes for new firmware, or contact your distributor for help.
  • The “Factory_Default_Config.cfg” can be used as the source to copy from, but cannot be used as the destination.
  • Although the switch supports only two operation code files, the maximum number of user-defined configuration files supported is 16.

Examples
nx9500-6C8809#adopted upgrade tftp://192.168.0.99/ex3500-adopted-5.8.1.0.img on ex3524-ED5EAC
Flash programming started
Flash programming completed
Successful
nx9500-6C8809#

nx9500-6C8809#ex3500 copy tftp file 10.2.0.100 1 m360.bix m360.bix on ex3524-ED5EAC
\Write to FLASH Programming.
\Write to FLASH finish.
Success.
nx9500-6C8809#

nx9500-6C8809#ex3500 copy tftp startup-config 10.2.0.99 startup.01 startup on ex3524-ED5EAC
TFTP server ip address: 10.1.0.99
Flash programming started.
Flash programming completed.
Success.
nx9500-6C8809#
### 3.1.28 factory-reset

#### Privileged Exec Mode Commands

Erases startup configuration on a specified device or all devices within a specified RF Domain

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

- `factory-reset <HOSTNAME/MAC>`
- `factory-reset on <RF-DOMAIN-NAME>`
- `factory-reset [config-all|config-device-only] on <RF-DOMAIN-NAME>`

#### Parameters

- **factory-reset <HOSTNAME/MAC>**
  - Erases startup configuration and reloads device(s) based on the parameters passed
  - For more information on the actions performed by this command, see *Actions performed by the factory-reset command.*

- **<HOSTNAME/MAC>**
  - Erases startup configuration and reloads the device identified by the `<HOSTNAME/MAC>` keyword. Specify the device’s hostname or MAC address.
  - **<HOSTNAME/MAC>** – Optional. You can optionally specify multiple space-separated devices.

- **factory-reset on <RF-DOMAIN-NAME>**
  - Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain identified by the `<RF-DOMAIN-NAME>` keyword
  - For more information on the actions performed by this command, see *Actions performed by the factory-reset command.*

- **on <RF-DOMAIN-NAME>**
  - Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain identified by the `<RF-DOMAIN-NAME>` keyword
  - **<RF-DOMAIN-NAME>** – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are:
    - **containing <SUB-STRING>** – Optional. Executes the command on all devices containing a specified sub-string in their hostname
    - **<SUB-STRING>** – Specify the sub-string to match.
    - **exclude-controllers** – Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.
    - **exlude-rf-domain-manager** – Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.
    - **filter <DEVICE-TYPE>**

Contd..
### factory-reset

Erases startup configuration and reloads device(s) based on the parameters passed.

For more information on the actions performed by this command, see **Actions performed by the factory-reset command.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>factory-reset</strong></td>
<td>Erases startup configuration and reloads device(s) based on the parameters passed.</td>
</tr>
<tr>
<td>[config-all</td>
<td>configure-device-only]</td>
</tr>
<tr>
<td><strong>&lt;HOSTNAME/MAC&gt;</strong></td>
<td>Erases startup configuration and reloads the device identified by the <code>&lt;HOSTNAME/MAC&gt;</code> keyword. Specify the device’s hostname or MAC address.</td>
</tr>
<tr>
<td><strong>&lt;HOSTNAME/MAC&gt;</strong></td>
<td>Optional. You can optionally specify multiple space-separated devices.</td>
</tr>
<tr>
<td>**on &lt;RF-DOMAIN-NAME&gt; {containing &lt;SUB-STRING&gt;</td>
<td>exclude-controllers</td>
</tr>
<tr>
<td>**on &lt;RF-DOMAIN-NAME&gt; {containing &lt;SUB-STRING&gt;</td>
<td>exclude-controllers</td>
</tr>
<tr>
<td><strong>&lt;RF-DOMAIN-NAME&gt;</strong></td>
<td>Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are:</td>
</tr>
<tr>
<td><strong>&lt;RF-DOMAIN-NAME&gt;</strong></td>
<td>containing &lt;SUB-STRING&gt; – Optional. Executes the command on all devices containing a specified sub-string in their hostname.</td>
</tr>
<tr>
<td><strong>&lt;RF-DOMAIN-NAME&gt;</strong></td>
<td><code>&lt;SUB-STRING&gt;</code> – Specify the sub-string to match.</td>
</tr>
<tr>
<td><strong>exclude-controllers</strong></td>
<td>Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.</td>
</tr>
<tr>
<td><strong>exclude-rf-domain-manager</strong></td>
<td>Optional. Executes the command on all devices excluding RF Domain managers. Use this option when executing the command on the NOC, Site controller, or RF Domain manager.</td>
</tr>
</tbody>
</table>

Contd..
Usage Guidelines

Actions performed by the `factory-reset` command.

The action taken by this command depends on the parameters passed.

- For the `factory-reset [DEVICE-NAME]|on <RF-DOMAIN-NAME>` options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.
  - Erases the device configuration entries from the controller’s configuration for the target device (or) for all the devices in the target RF Domain.
  - Reloads the target device (or) all devices in the target RF Domain.

- For the `factory-reset config-all [DEVICE-NAME]|on <RF-DOMAIN-NAME>` options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.
  - Erases the device configuration entries from the controller’s configuration for the target device (or) for all the devices in the target RF Domain.

- For the `factory-reset config-device-only [DEVICE-NAME]|on <RF-DOMAIN-NAME>` options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.

Examples

```bash
nx7500-7F3609# factory-reset config-all ap6522-5A873C
In progress ....
Erased startup-config - success 1 fail 0
Successful device deletion - total 1
nx7500-7F3609#
```

```bash
rfs6000-18072B# factory-reset ap650-72DBC4 ap650-72E53C
In progress ....
Erased startup-config and initiated reload - success 2 fail 0
Successful device deletion - total 2
rfs6000-18072B#
```

```bash
rfs6000-18072B# factory-reset B4-C7-99-5A-87-3C
In progress ....
Erased startup-config and initiated reload - success 1 fail 0
Successful device deletion - total 1
rfs6000-18072B#
```

The following example displays the access points in the RF Domain 'rfd1':

```bash
nx7500-7F3609# show wireless ap on rfd1
```

```
+-----------------+-----------------+--------+----------+----------+----------+--------+----------+----------+----------+
<table>
<thead>
<tr>
<th>AP-NAME</th>
<th>AP-LOCATION</th>
<th>RF-DOMAIN</th>
<th>AP-MAC</th>
<th>#RADIOS</th>
<th>MODE</th>
<th>#CLIENT</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap7131-1180FC</td>
<td>rfd1</td>
<td>00-23-68-11-80-FC</td>
<td>2 W-W</td>
<td>0</td>
<td>0.0.0.0</td>
<td>::</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap6522-551648</td>
<td>rfd1</td>
<td>B4-C7-99-55-16-48</td>
<td>2 W-W</td>
<td>0</td>
<td>0.0.0.0</td>
<td>::</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap8232-7F0DF8</td>
<td>rfd1</td>
<td>FC-0A-81-7F-0D-FC</td>
<td>2 W-W</td>
<td>0</td>
<td>0.0.0.0</td>
<td>::</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Total number of APs displayed: 3

nx7500-7F3609#
When the factory-reset command is executed on the RF Domain 'rfd1' with 'exclude-rf-domain-manager' the startup configuration:

- is erased on all non-domain-manager devices (ap7131-1180FC and ap6522-551648) within the RF Domain 'rfd1', but
- not erased on the RF Domain manager (ap8232-7F0DF8).

```
nx7500-7F3609# factory-reset config-device-only on rfd1 exclude-rf-domain-manager
In progress ....
Erased startup-config -
ap7131-1180FC: OK
ap6522-551648: OK

nx7500-7F3609#
nx7500-7F3609# factory-reset on rfd2
In progress ....
Erased startup-config and initiated reload -
ap650-A6566C: OK, Reload scheduled in 60 seconds...
ap4532-34505C: OK, Reload scheduled in 60 seconds...
ap650-345000: OK, Reload scheduled in 60 seconds...

Successful device deletion - total 3
nx7500-7F3609#```
3.1.29 file-sync

Privileged Exec Mode Commands

Syncs EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adoptee AP6522/AP6562 client-bridge access points. Use this command to configure parameters that enable syncing of PKCS#12 certificate.

When enabling file syncing, consider the following points:

• The X.509 certificate needs synchronization only if the access point’s radio2, the client-bridge radio, is configured to use EAP-TLS authentication
• Execute the command on the controller adopting the access point
• Ensure that the X.509 certificate file is installed on the controller
• If the adopting device is a site controller with layer 3 adoption to the NOC, ensure that the X.509 certificate is synced across the hierarchically managed setup – between the NOC, site-controller (the staging-controller), and the client-bridge access points.

Syncing of wireless client-bridge certificate can be automated. To automate the file syncing process, in the controller’s device/profile configuration mode, execute the following command: file-sync [auto|count <1-20>]. For more information, see file-sync.

For more information on configuring an AP client-bridge, see bridge.

Supported in the following platforms:

• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

file-sync [cancel|load-file|wireless-bridge]

file-sync cancel wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]

file-sync load-file wireless-bridge <URL>

file-sync wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all] {from-controller] {reset-radio|upload-time <TIME>}

Parameters

• file-sync cancel wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]

| file-sync cancel wireless-bridge [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]] | Cancels scheduled wireless client-bridge certificate synchronization on a specified AP, or all APs, or APs within an RF Domain |
|-----------------------------------------------|-------------------------------------------------------------|
| • <DEVICE-NAME> – Cancels scheduled certificate synchronization on the AP identified by the <DEVICE-NAME> parameter. Specify the AP’s hostname or MAC address. |
| • all – Cancels scheduled certificate synchronization on all APs |
| • rf-domain [<DOMAIN-NAME>|all] – Cancels scheduled certificate synchronization on all APs in a specified RF Domain or in all RF Domains |
| • <DOMAIN-NAME> – Cancels scheduled certificate synchronization on all APs within the RF Domain identified by the <DOMAIN-NAME> parameter. Specify the RF Domain’s name. |
| • all – Cancels scheduled certificate synchronization on all RF Domains |
• **file-sync load-file wireless-bridge <URL>**

**file-sync load-file wireless-bridge <URL>**

Loads the wireless client-bridge certificate to the staging controller. Use this command to load the certificate to the controller before scheduling or initiating a certificate synchronization.

- `<URL>` – Provide the certificate location using one of the following formats:
  - tftp://<hostname/IP>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname/IP>[:port]/path/file
  - sftp://<user>:<passwd>@<hostname/IP>[:port]/path/file
  - http://<hostname/IP>[:port]/path/file
  - cf:/path/file
  - usb<n>:/path/file

**Note:** Both IPv4 and IPv6 address types are supported.

• **file-sync wireless-bridge [ DEVICE-NAME ] [ all ] rf-domain [ DOMAIN-NAME ] [ all ] from-controller [ ] { reset-radio | upload-time <TIME> }**

**file-sync wireless-bridge [ DEVICE-NAME ] [ all ] rf-domain [ DOMAIN-NAME ] [ all ] from-controller [ ] { reset-radio | upload-time <TIME> }**

Configures the following file-sync parameters:

- post certificate synchronization action
- upload time

These file-sync options can be applied to a specified AP, all APs, or all APs within a specified RF Domain or on all RF Domains.

- `<DEVICE-NAME>` – Applies these parameters to the AP identified by the `<DEVICE-NAME>` parameter. Specify the AP’s hostname or MAC address.
- `all` – Applies these parameters to all APs
- `rf-domain [ DOMAIN-NAME ] [ all ]` – Applies these parameters to all APs in a specified RF Domain or in all RF Domains
  - `<DOMAIN-NAME>` – Select to apply to APs within the RF Domain identified by the `<DOMAIN-NAME>` parameter. Specify the RF Domain’s name.
  - `all` – Select to apply these parameters to APs in all RF Domains
  - `from-controller` – Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager

After specifying the access points to load certificate, specify the following options: reset-radio and upload-time.

**reset-radio**

This keyword is recursive and applicable to all of the above parameters.

Optional. Resets the radio after file synchronization

**upload-time <TIME>**

This keyword is recursive and applicable to all of the above parameters.

Optional. Schedules file upload at a specified time

- `<TIME>` – Specify the time in the MM/DD/YYYY-HH:MM or HH:MM format. If no time is configured, the process is initiated as soon as the command is executed.

**Examples**

rfs7000-6DCD4B# file-sync wireless-bridge ap7131-11E6C4 upload-time 12/12/2015-12:30

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-CD-4B</td>
<td>Success</td>
<td>Queued 1 APs to upload</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B#
3.1.30 **format**

*Privileged Exec Mode Commands*

Formats a device’s compact flash file system

Supported in the following platforms:

- Wireless Controllers — RFS7000

**Syntax**

`format cf:`

**Parameters**

- `format cf:`

| cf: | Formats the compact flash file system |

**Examples**

`rfs7000-37FABE#format cf:`

Warning: This will destroy the contents of compact flash.
Do you want to continue [y/n]? n

`rfs7000-37FABE`
### 3.1.31 halt

**Privileged Exec Mode Commands**

Stops (halts) a device (access point, wireless controller, or service platform). Once halted, the system must be restarted manually.

This command stops the device immediately. No indications or notifications are provided while the device shuts down.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
halt {force} {(on <DEVICE-NAME>)}
```

**Parameters**

- **halt** {force} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>halt</td>
<td>Halts a device</td>
</tr>
<tr>
<td>force</td>
<td>Optional. Forces a device to halt ignoring in-progress operations, such as firmware upgrades, downloads, unsaved configuration changes, etc.</td>
</tr>
</tbody>
</table>
| on <DEVICE-NAME> | The following keywords are recursive and applicable to the ‘force’ parameter:  
  - on <DEVICE-NAME> – Optional. Specifies the name of the device to be halted  
  - <DEVICE-NAME> – Enter the name of the AP, wireless controller, or service platform.  
  **Note:** If the device name is not specified, the logged device is halted. |

**Examples**

```
rfs7000-37FABE#halt on rfs7000-37FABE
rfs7000-37FABE#
```
### 3.1.32 join-cluster

#### Privileged Exec Mode Commands

Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
join-cluster <IP> user <USERNAME> password <WORD> {level|mode}
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode [active|standby]}
```

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>Specify the cluster member's IP address.</td>
</tr>
<tr>
<td>user &lt;USERNAME&gt;</td>
<td>Specify a user account with super user privileges on the new cluster member.</td>
</tr>
<tr>
<td>password &lt;WORD&gt;</td>
<td>Specify password for the account specified in the user parameter.</td>
</tr>
<tr>
<td>level [1</td>
<td>2]</td>
</tr>
<tr>
<td>mode [active</td>
<td>standby]</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

To add a device to an existing cluster:
- Configure a static IP address on the device (access point, wireless controller, or service platform).
- Provide username and password for superuser, network admin, system admin, or operator accounts.

After adding the device to a cluster, execute the “write memory” command to ensure the configuration persists across reboots.

#### Examples

```
rfs6000-6DB5D4#join-cluster 192.168.13.16 user admin password superuser level 1
  mode standby
  ... connecting to 192.168.13.16
  ... applying cluster configuration
  ... committing the changes
  ... saving the changes
  [OK]
rfs6000-6DB5D4#
```

```
rfs6000-6DB5D4#show context
  !
  ! Configuration of RFS6000 version 5.8.1.0-021D
  !
  ! version 2.3
  !
```
interface ge1
   switchport mode access
   switchport access vlan 1
interface vlan1
   ip address 192.168.13.16/24
   ip dhcp client request options all
   no ipv6 enable
   no ipv6 request-dhcpv6-options
cluster name TechPubs
cluster mode standby
cluster member ip 192.168.13.16 level 1
logging on
logging console warnings
logging buffered warnings
!
!
end
rfs6000-6DB5D4#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Initiates the cluster context. The cluster context provides centralized management to configure all cluster members from any one member.</td>
</tr>
<tr>
<td>create-cluster</td>
<td>Creates a new cluster on a specified device</td>
</tr>
</tbody>
</table>
### 3.1.33 l2tpv3

**Privileged Exec Mode Commands**

Establishes or brings down an L2TPv3 tunnel

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
12tpv3 tunnel [<TUNNEL-NAME>|all]
12tpv3 tunnel <TUNNEL-NAME> [down|session|up] {on <DEVICE-NAME>}
12tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}
12tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

**Parameters**

- **l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
  - Establishes or brings down an L2TPv3 tunnel
  - `<TUNNEL-NAME>` – Specify the tunnel name.
  - `down` – Brings down the specified tunnel
  - `up` – Establishes the specified tunnel
  - `on <DEVICE-NAME>` Optional. Establishes or brings down a tunnel on a specified device

- **l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}
  - Establishes or brings down a session in the specified tunnel
  - `<TUNNEL-NAME>` – Specify the tunnel name.
  - `<SESSION-NAME>` – Specify the session name.
  - `down` – Brings down the specified tunnel session
  - `up` – Establishes the specified tunnel session
  - `on <DEVICE-NAME>` Optional. Establishes or brings down a tunnel session on a specified device

- **l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
  - Establishes or brings down all L2TPv3 tunnels
  - `down` – Brings down all tunnels
  - `up` – Establishes all tunnels
  - `on <DEVICE-NAME>` Optional. Establishes or brings down all tunnels on a specified device

---

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12tpv3 tunnel &lt;TUNNEL-NAME&gt; [down</td>
<td>up] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>12tpv3 tunnel &lt;TUNNEL-NAME&gt; session &lt;SESSION-NAME&gt; [down</td>
<td>up] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>12tpv3 tunnel all [down</td>
<td>up] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
</tbody>
</table>
```
Examples

rfs7000-37FABE#l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on rfs7000-37FABE

NOTE: For more information on the L2TPv3 tunnel configuration mode and commands, see Chapter 22, L2TPV3-POLICY.
3.1.34 logging

Privileged Exec Mode Commands

Modifies message logging settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

logging monitor \{<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings\}

Parameters

- logging monitor \{<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings\}

monitor

Sets terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system configures default settings, if no logging severity level is specified.

- \(<0-7>\) – Optional. Enter the logging severity level from 0 - 7. The various levels and their implications are:
  - alerts – Optional. Immediate action needed (severity=1)
  - critical – Optional. Critical conditions (severity=2)
  - debugging – Optional. Debugging messages (severity=7)
  - emergencies – Optional. System is unusable (severity=0)
  - errors – Optional. Error conditions (severity=3)
  - informational – Optional. Informational messages (severity=6)
  - notifications – Optional. Normal but significant conditions (severity=5)
  - warnings – Optional. Warning conditions (severity=4)

Note: Ensure that the logging module is enabled, before configuring the message logging level. To enable message logging, in the device’s configuration mode, execute the logging > on command. Message logging can also be enabled on a profile.

Examples

rfs4000-229D58(config-device-00-23-68-22-9D-58)#logging on

rfs4000-229D58#logging monitor debugging

rfs4000-229D58#show logging

Logging module: enabled
Aggregation time: disabled
Console logging: level debugging
Monitor logging: level debugging
Buffer logging: level warnings
Syslog logging: level warnings
Facility: local7

Log Buffer (804 bytes):

May 30 11:23:13 2015: rfs4000-229D58 : %NSM-4-IFUP: Interface ge4 is up
May 30 11:23:11 2015: rfs4000-229D58 : %NSM-4-IFUP: Interface ge4 is up
May 30 11:22:15 2015: rfs4000-229D58 : %NSM-4-IFDOWN: Interface ge4 is down
May 30 08:41:59 2015: rfs4000-229D58 : %NSM-4-IFUP: Interface ge4 is up
May 30 08:41:58 2015: rfs4000-229D58 : %NSM-4-IFUP: Interface ge4 is up
May 29 11:41:17 2015: rfs4000-229D58 : %NSM-4-IFUP: Interface ge4 is up
May 29 11:41:16 2015: rfs4000-229D58 : %NSM-4-IFUP: Interface ge4 is up
rfs4000-229D58#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets terminal lines logging levels</td>
</tr>
</tbody>
</table>
### 3.1.35 mint

**Privileged Exec Mode Commands**

Uses MiNT protocol to perform a ping and traceroute to a remote device

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

- mint [ping|traceroute]
- mint ping <MINT-ID> {count <1-10000>|size <1-64000>|timeout <1-10>}
- mint traceroute <MINT-ID> {destination-port <1-65535>|max-hops <1-255>|source-port <1-65535>|timeout <1-255>}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping &lt;MINT-ID&gt;</td>
<td>Sends a MiNT echo message to a specified destination</td>
</tr>
<tr>
<td>count &lt;1-10000&gt;</td>
<td>Optional. Sets the pings to the MiNT destination</td>
</tr>
<tr>
<td>size &lt;1-64000&gt;</td>
<td>Optional. Sets the MiNT payload size in bytes</td>
</tr>
<tr>
<td>timeout &lt;1-10&gt;</td>
<td>Optional. Sets a response time in seconds</td>
</tr>
<tr>
<td>traceoute &lt;MINT-ID&gt;</td>
<td>Prints the route packets trace to a device</td>
</tr>
<tr>
<td>destination-port &lt;1-65535&gt;</td>
<td>Optional. Sets the Equal-cost Multi-path (ECMP) routing destination port</td>
</tr>
<tr>
<td>max-hops &lt;1-255&gt;</td>
<td>Optional. Sets the maximum number of hops a traceroute packet traverses</td>
</tr>
<tr>
<td>source-port &lt;1-65535&gt;</td>
<td>Optional. Sets the ECMP source port</td>
</tr>
<tr>
<td>timeout &lt;1-255&gt;</td>
<td>Optional. Sets the minimum response time period</td>
</tr>
</tbody>
</table>
Examples

rfs4000-229D58#mint ping 68.88.0D.A7
MiNT ping 68.88.0D.A7 with 64 bytes of data.
   Response from 68.88.0D.A7: id=1 time=0.364 ms
   Response from 68.88.0D.A7: id=2 time=0.333 ms
   Response from 68.88.0D.A7: id=3 time=0.368 ms

--- 68.88.0D.A7 ping statistics ---
 3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.333/0.355/0.368 ms
rfs4000-229D58#
3.1.36 mkdir

Privileged Exec Mode Commands

Creates a new directory in the file system

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
mkdir <DIR>

Parameters
- mkdir <DIR>

Examples

rfs4000-229D58#dir
Directory of flash:/.

    drwx Mon Jun 9 05:13:12 2014   log
    drwx Sat Jan 1 05:30:09 2000   configs
    drwx Sat Jan 1 05:30:08 2000   cache
    drwx Mon May 5 04:50:06 2014   crashinfo
    drwx Mon Jun 9 05:09:57 2014   archived_logs
    drwx Sat Jan 1 05:30:08 2000   upgrade
    drwx Sat Jan 1 05:30:09 2000   hotspot
    drwx Sat Jan 1 05:30:09 2000   floorplans
    -rw- 137728 Thu Jun 5 09:41:00 2014   in.tar
    drwx Sat Jan 1 05:30:09 2000   startuplog
    -rw- 176128 Fri Feb 15 20:02:51 2013   out.tar

rfs4000-229D58#

rfs4000-229D58#mkdir test

rfs4000-229D58#dir
Directory of flash:/.

    drwx Mon Jun 9 05:13:12 2014   log
    drwx Tue Jun 10 08:58:13 2014   test
    drwx Sat Jan 1 05:30:09 2000   configs
    drwx Sat Jan 1 05:30:08 2000   cache
    drwx Mon May 5 04:50:06 2014   crashinfo
    drwx Mon Jun 9 05:09:57 2014   archived_logs
    drwx Sat Jan 1 05:30:08 2000   upgrade
    drwx Sat Jan 1 05:30:09 2000   hotspot
    drwx Sat Jan 1 05:30:09 2000   floorplans
    -rw- 137728 Thu Jun 5 09:41:00 2014   in.tar
    drwx Sat Jan 1 05:30:09 2000   startuplog
    -rw- 176128 Fri Feb 15 20:02:51 2013   out.tar

rfs4000-229D58#
Privileged Exec Mode Commands

Displays files on the device’s file system. This command navigates and displays specific files in the device’s file system. Provide the complete path to the file more <file>.

The more command also displays the startup configuration file.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

more <FILE>

Parameters

- more <FILE>

Examples

rfs4000-229D58#more flash:/archived_logs/startup.1.log
23-38-04-06-08-14
Mar 16 05:07:15 2015: %PM-6-PROCSTART: Starting process "/usr/sbin/logd"
Mar 16 05:07:15 2015: %PM-6-PROCSTART: Starting process "/usr/sbin/isDiag"
Mar 16 05:07:21 2015: %PM-6-PROCSTART: Starting process "/usr/sbin/rim"
Mar 16 05:07:42 2015: %PM-6-PROCSTART: Starting process "/etc/init.d/cfgd"
Mar 16 05:07:44 2015: %PM-6-PROCSTART: Starting process "/usr/sbin/ssm"
Mar 16 05:07:45 2015: %KERN-6-INFO: ge1 { no link }.
Mar 16 05:07:44 2015: %PM-6-PROCSTART: Starting process "/usr/sbin/nsm"
Mar 16 05:07:45 2015: %PM-6-PROCSTART: Starting process "/etc/init.d/dpd2.init"
Mar 16 05:07:45 2015: %PM-6-PROCSTART: Starting process "/usr/sbin/had"
--More--
rfs4000-229D58#
Privileged Exec Mode Commands

Use the no command to revert a command or a set of parameters to their default. This command is useful to turn off an enabled feature or to revert to default settings.

The no commands have their own set of parameters that can be reset. These parameters depend on the context in which the command is being used.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
no [adoption|captive-portal|cpe|crypto|debug|logging|page|raid|service|
    terminal|upgrade|virtual-machine|wireless]
no adoption {on <DEVICE-OR-DOMAIN-NAME>}
no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>] {on <DEVICE-OR-DOMAIN-NAME>}
no crypto pki [server|trustpoint] {del-key {on <DEVICE-NAME>} | on <DEVICE-NAME>}
no logging monitor
no page
no service [block-adopter-config-update|locator|snmp|ssm|wireless]
no service block-adopter-config-update
no service locator {on <DEVICE-NAME>}
no service snmp sysoid wing5
no service ssm trace pattern {<WORD>} {(on <DEVICE-NAME>)}
no service wireless [trace pattern {<WORD>} {(on <DEVICE-NAME>)}| unsanctioned ap air-terminate <BSSID> {on <DOMAIN-NAME>}]
no terminal [length|width]
no upgrade <PATCH-NAME> {on <DEVICE-NAME>}
no wireless client [all|<MAC>] {filter|on}
no wireless client all {filter [wlan <WLAN-NAME>]}
no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}
no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
```

The following command is available only on the RFS4000, RFS7000, NX45XX, NX65XX, and NX9000 series service platforms:

```
no cpe led cpe [<1-24>|all] {on <T5-DEVICE-NAME>}
```
The following command is available only on the NX45XX, NX65XX, and NX9000 series service platforms:

```
no virtual-machine assign-usb-ports {on <DEVICE-NAME>}
```

The following commands are available only on the NX9000 series service platforms:

```
no raid locate
```

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Resets or reverts settings based on the parameters passed |

**Usage Guidelines**

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

**Examples**

```
rfs7000-37FABE# no adoption
rfs7000-37FABE#
```

```
rfs7000-37FABE# no page
rfs7000-37FABE#
```
3.1.39 on

Privileged Exec Mode Commands

Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

on rf-domain [<RF-DOMAIN-NAME>|all]

Parameters

- on rf-domain [<RF-DOMAIN-NAME>|all]

| on rf-domain [<RF-DOMAIN-NAME>|all] | Enter the RF Domain context based on the parameter specified |
|--------------------------------------|-----------------------------------------------------------|
|                                    | • <RF-DOMAIN-NAME> – Specify the RF Domain name. Enters the specified RF Domain context. |
|                                    | • all – Specifies all RF Domains. |

Examples

nx9500-6C8809# on rf-domain TechPubs
nx9500-6C8809(TechPubs)#

nx9500-6C8809(TechPubs)#?

on RF-Domain Mode commands:

<table>
<thead>
<tr>
<th></th>
<th>clrscr</th>
<th>clears the display screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td></td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td></td>
</tr>
</tbody>
</table>

nx9500-6C8809(TechPubs)#?

nx9500-6C8809(TechPubs)# show adoption timeline on default/ap7532-80C2AC

<table>
<thead>
<tr>
<th>AP-NAME</th>
<th>RF-DOMAIN</th>
<th>LAST-ADOPTION-TIMESTAMP</th>
<th>ADOPTED-SINCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>nx4500-5CFA2B</td>
<td>default</td>
<td>2015-04-08 09:50:02</td>
<td>9 days 01:13:54</td>
</tr>
<tr>
<td>nx4500-5CFA8E</td>
<td>default</td>
<td>2015-04-08 09:49:48</td>
<td>9 days 01:14:08</td>
</tr>
</tbody>
</table>

Total number of devices displayed: 2

nx9500-6C8809(TechPubs)#
**3.1.40 opendns**

> Privileged Exec Mode Commands

Retrieves the OpenDNS device-id from the OpenDNS site

This command integrates access points and controllers with OpenDNS. It obtains the device-id (16 character hex-string) from OpenDNS. This device-id is configured under all WLANs that are to be OpenDNS enabled. When configured and enabled on a WLAN, DNS queries from all wireless clients on the WLAN are redirected to OpenDNS (208.67.220.220 or 208.67.222.222) resolvers. These OpenDNS resolvers act as proxy DNS servers, and also provide additional features, such as Web filtering, performance improvements etc.

**NOTE:** OpenDNS is a free, alternative DNS service that is faster and more reliable than other DNS services available. OpenDNS enables swift navigation of the Web without the outages that are frequent in other ISP provided DNS services. It also blocks inappropriate Web sites, phishing sites, and prevents virus and malware attacks.

**NOTE:** The 'username' and 'password' values passed in this command should be pre-registered with the OpenDNS site. The 'label' can be any value. Only with a combination of a valid 'username', 'password', and any 'label' the OpenDNS server returns a device-id.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>

**Parameters**

- opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>opendns</td>
<td>Obtains the OpenDNS device-id from the OpenDNS site</td>
</tr>
<tr>
<td>username</td>
<td>Configures the OpenDNS user name (should be valid username registered with OpenDNS)</td>
</tr>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>• &lt;USERNAME&gt; – Provide the OpenDNS user name.</td>
</tr>
<tr>
<td>password</td>
<td>Configures the password associated with the user configured in the previous step</td>
</tr>
<tr>
<td>&lt;OPENDNS-PSWD&gt;</td>
<td>• &lt;OPENDNS-PSWD&gt; – Provide the OpenDNS password for the user.</td>
</tr>
<tr>
<td>label</td>
<td>Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal.</td>
</tr>
<tr>
<td>&lt;LABEL&gt;</td>
<td>• &lt;LABEL&gt; – Specify your network label.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For every unique set of username, password, and label only one device-id is returned. Apply this device-id in WLANs that are to be OpenDNS enabled. For information on configuring the device-id in the WLAN context, see <strong>opendns</strong>.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use your OpenDNS credentials to logon to the opendns.org site and use the labels, edit settings, and customize content filtering options to configure Web filtering settings.

Examples

ap7131-E6D512#opendns username bob@examplecompany.com password opendns label company_name
Connecting to OpenDNS server...
device_id = 0014AADP8EDC6CS9
ap7131-E6D512#
3.1.41 page

Privileged Exec Mode Commands

Toggles controller paging. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

page

Parameters

None

Examples

rfs7000-37FABE:#page
rfs7000-37FABE#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables controller paging</td>
</tr>
</tbody>
</table>
3.1.42 ping

Privileged Exec Mode Commands

Sends Internet Controller Message Protocol (ICMP) echo messages to a user-specified location.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|source [<IP]|pppoe|vlan <1-4094>|wwan}]
```

Parameters

- `<IP/HOSTNAME>` Specify the destination IP address or hostname to ping. When entered without any parameters, this command prompts for an IP address or a hostname.
- `count <1-10000>` Optional. Sets the pings to the specified destination.
  - `<1-10000>` – Specify a value from 1 - 10000. The default is 5.

- `dont-fragment {count|size}` Optional. Sets the dont-fragment bit in the ping packet. Packets with the dont-fragment bit specified, are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified Maximum Transmission Unit (MTU) value, an error message is sent from the device trying to fragment it.
  - `count <1-10000>` – Sets the pings to the specified destination from 1 - 10000. The default is 5.
  - `size <1-64000>` – Sets the size of ping payload size from 1 - 64000 bytes. The default is 100 bytes.

- `size <1-64000>` Optional. Sets the ping packet’s size in bytes.
  - `<1-64000>` – Specify the ping payload size from 1 - 64000 bytes. The default is 100 bytes.

- `source [<IP]|pppoe|vlan <1-4094>|wwan]` Optional. Sets the source address or interface name. This is the source of the ICMP packet to the specified destination.
  - `<IP>` – Specifies the source IP address
  - `pppoe` – Selects the PPP over Ethernet interface
  - `vlan <1-4094>` – Selects the VLAN interface from 1 - 4094
  - `wwan` – Selects the wireless WAN interface
Examples

rfs7000-37FABE#ping 172.16.10.4 count 6
PING 172.16.10.4 (172.16.10.4) 100(128) bytes of data.
108 bytes from 172.16.10.4: icmp_seq=1 ttl=64 time=3.93 ms
108 bytes from 172.16.10.4: icmp_seq=2 ttl=64 time=0.367 ms
108 bytes from 172.16.10.4: icmp_seq=3 ttl=64 time=0.328 ms
108 bytes from 172.16.10.4: icmp_seq=4 ttl=64 time=0.295 ms
108 bytes from 172.16.10.4: icmp_seq=5 ttl=64 time=0.340 ms
108 bytes from 172.16.10.4: icmp_seq=6 ttl=64 time=0.371 ms
--- 172.16.10.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.295/0.939/3.936/1.340 ms
rfs7000-37FABE#

rfs7000-6DCD4B#ping 10.2.0.99 source 172.18.0.2
PING 10.2.0.99 (10.2.0.99) from 172.18.0.2 : 100(128) bytes of data.
108 bytes from 10.2.0.99: icmp_seq=1 ttl=63 time=1.16 ms
108 bytes from 10.2.0.99: icmp_seq=2 ttl=63 time=0.744 ms
108 bytes from 10.2.0.99: icmp_seq=3 ttl=63 time=0.648 ms
108 bytes from 10.2.0.99: icmp_seq=4 ttl=63 time=0.662 ms
108 bytes from 10.2.0.99: icmp_seq=5 ttl=63 time=0.651 ms
--- 10.2.0.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.648/0.774/1.168/0.202 ms
rfs7000-6DCD4B#
3.1.43 ping6

Privileged Exec Mode Commands

Sends ICMPv6 echo messages to a user-specified IPv6 address

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>|count <1-10000>|size <1-64000>}
```

Parameters

- ping <IPv6/HOSTNAME> {<INTF-NAME>|count <1-10000>|size <1-64000>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPv6/HOSTNAME&gt;</td>
<td>Specify the destination IPv6 address or hostname.</td>
</tr>
<tr>
<td>&lt;INTF-NAME&gt;</td>
<td>Optional. Specify the interface name for link local/broadcast address</td>
</tr>
<tr>
<td>count &lt;1-10000&gt;</td>
<td>Optional. Sets the pings to the specified IPv6 destination</td>
</tr>
<tr>
<td>size &lt;1-64000&gt;</td>
<td>Optional. Sets the IPv6 ping payload size in bytes</td>
</tr>
</tbody>
</table>

Usage Guidelines

To configure a device’s IPv6 address, in the VLAN interface configuration mode, use the `ipv6 > address <IPv6-ADDRESS> command`. After configuring the IPv6 address, use the `ipv6 > enable` command to enable IPv6. For more information see, `ipv6`.

Examples

```
rfs4000-1B3596#ping6 2001:10:10:10:10:10:10:2 count 6 size 200
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=1 ttl=64 time=0.509 ms  
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=2 ttl=64 time=0.323 ms  
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=3 ttl=64 time=0.318 ms  
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=4 ttl=64 time=0.317 ms  
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=5 ttl=64 time=0.314 ms  
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=6 ttl=64 time=0.318 ms  
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.314/0.349/0.509/0.075 ms
rfs4000-1B3596# ```
3.1.44 pwd

Privileged Exec Mode Commands

Displays the full path of the present working directory, similar to the UNIX pwd command

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

pwd

Parameters

None

Examples

rfs4000-229D58#pwd
flash:/
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

drwx Thu Apr 16 04:03:34 2015 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Sat Jan 1 05:30:08 2000 cache
drwx Mon Jan 27 04:08:32 2014 crashinfo
drwx Thu Apr 16 04:00:27 2015 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:08 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 startuplog

rfs4000-229D58#
### 3.1.45 re-elect

**Privileged Exec Mode Commands**

Re-elects the tunnel controller (wireless controller or service platform)

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

**Parameters**
- `re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>re-elect tunnel-controller</th>
<th>Re-elects the tunnel controller</th>
</tr>
</thead>
</table>
| `<WORD>` {on <DEVICE-NAME>}` | Optional. Re-elects the tunnel controller on all devices whose preferred tunnel controller name matches `<WORD>`
  - `{on <DEVICE-NAME>}` – Optional. Re-elects the tunnel controller on a specified device
  - `{on <DEVICE-NAME>}` – Specify the name of the AP, wireless controller, or service platform.

**Examples**

```plaintext
rfs7000-37FABE#re-elect tunnel-controller
OK
rfs7000-37FABE#
```
3.1.46 reload

Privileged Exec Mode Commands

Halts a device or devices and performs a warm reboot

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
reload {<DEVICE-MAC-OR-HOSTNAME>|at|cancel|force|in|on|staggered}
reload {((<DEVICE-MAC-OR-HOSTNAME>)}
reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}
reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}
reload {force} {((<DEVICE-MAC-OR-HOSTNAME>)|on <DOMAIN-NAME>|staggered})
reload {force} {on <DOMAIN-NAME> {staggered}|staggered {<DEVICE-MAC-OR-HOSTNAME>}|filter <DEVICE-TYPE>}
reload {in <1-999>} {list|on}
reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}
reload {in <1-999>} {on <DEVICE-OR-DOMAIN-NAME>}
reload {on <DOMAIN-NAME>} {containing <WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}
reload {staggered} {((<DEVICE-MAC-OR-HOSTNAME>)|on <DOMAIN-NAME>) {containing <WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}

Parameters
- reload {((<DEVICE-MAC-OR-HOSTNAME>)
- reload <DEVICE-MAC-OR-HOSTNAME> Initiates device(s) reloads and configures associated parameters
  The following keyword is recursive and allows you to specify multiple devices:
  - <DEVICE-MAC-OR-HOSTNAME> – Optional. Reloads a specified device(s), identified by the <DEVICE-MAC-OR-HOSTNAME> keyword. Specify the device's hostname or MAC address.
  Note: If no device is specified, the system reloads the logged device.
- reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}
- reload at Initiates device(s) reloads and configures associated parameters
  - at – Optional. Schedules a reload at a specified time and day. Use the following keywords to specify the time and day: <TIME>, <1-31>, <MONTH>, and <1993-2035>.
  - <TIME> Specifies the time in the HH:MM:SS format
  - <1-31> Specifies the day of the month from 1 - 31
  - <MONTH> Specifies the month from Jan - Dec
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1993-2035&gt;</code></td>
<td>Specifies the year from 1993 - 2035. It should be a valid 4 digit year.</td>
</tr>
</tbody>
</table>
| `on <DEVICE-OR-DOMAIN-NAME>` | Optional. Performs reload at the scheduled time, on a specified device or all devices within a specified RF Domain. 
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain. When a RF Domain name is provided, all devices within the specified RF Domain are reloaded at the scheduled time. 
Note: If no device is specified, the reload is scheduled on the logged device. |
| `reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}` | Cancels pending/scheduled reloads of device(s). 
  - `cancel` – Optional. Cancels all pending reloads. 
  - `on <DEVICE-OR-DOMAIN-NAME>` – Optional. Cancels reloads pending on a specified device or all devices within a specified RF Domain. 
Note: If no device is specified, the system cancels reloads pending on the logged device. |
| `reload force` | Initiates device(s) reloads and configures associated parameters. 
  - `force` – Optional. Forces device(s) to reload, while ignoring conditions like upgrade in progress, unsaved changes etc. Use the options provided to force a reload on a specified device or all devices in a RF Domain. |
| `<DEVICE-MAC-OR-HOSTNAME>` | This keyword is recursive and allows you to specify multiple devices. 
  - `<DEVICE-MAC-OR-HOSTNAME>` – Optional. Forces a reload on a specified device identified by the `<DEVICE-MAC-OR-HOSTNAME>` keyword. Specify the device’s hostname or MAC address. When executed, the specified device(s) are forced to halt and a warm reboot is performed. 
Note: If no device is specified, the system forcefully reloaded the logged device. |
| `on <DOMAIN-NAME>` {staggered}|staggered {<DEVICE-MAC-OR-HOSTNAME>}|{containing <WORD>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}` | Initiates device(s) reloads and configures associated parameters. 
  - `force` – Optional. Forces device(s) to reload, while ignoring conditions like upgrade in progress, unsaved changes etc. Use the options provided to force a reload on a specified device or all devices in a RF Domain. 
  - `<DOMAIN-NAME>` – Optional. Specifies the name of the RF Domain. When executed, all devices within the specified RF Domain are forced to halt and a warm reboot is performed. 
  - `staggered` – Optional. Enables staggered reload of devices (one at a time) without network impact. Use this option when rebooting multiple devices within an RF Domain. When executed, all devices within the specified RF Domain are forced to halt and reboot in a staggered manner. |
### Staggered Reload


devices specified by the `<DEVICE-MAC-OR-HOSTNAME>` keyword. Specify the device’s hostname or MAC address. This is a recursive keyword that allows you to specify multiple devices. When executed, the specified device(s) are forced to halt and a warm reboot is performed.

- `<DEVICE-MAC-OR-HOSTNAME>` – Optional. Forces a reload on specified device(s) identified by the `<DEVICE-MAC-OR-HOSTNAME>` keyword. Specify the device’s hostname or MAC address. This is a recursive keyword that allows you to specify multiple devices. When executed, the specified device(s) are forced to halt and a warm reboot is performed.

### Optional Reload

- `<DOMAIN-NAME>` – Optional. Forces a reload on all devices in a RF Domain. Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are forced to halt and a warm reboot is performed.

**Note:** If no device or RF Domain is specified, the system forcefully reloads the logged device.

### Reload Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>reload</code></td>
<td>Initiates device(s) reloads and configures associated parameters</td>
</tr>
<tr>
<td><code>{in &lt;1-999&gt;}</code></td>
<td>Performs a reload after a specified time period</td>
</tr>
<tr>
<td>`{list {&lt;LINE&gt;</td>
<td>all}</td>
</tr>
<tr>
<td><code>&lt;LINE&gt;</code></td>
<td>Reloads listed devices. List all devices (to be reloaded) separated by a space.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Reloads all devices adopted by this controller</td>
</tr>
<tr>
<td><code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>Reloads a specified device or all devices within a specified RF Domain</td>
</tr>
<tr>
<td><code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

**Note:** If no RF Domain is specified, the system reloads the logged device.
<table>
<thead>
<tr>
<th>Command Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>When reloading devices in a RF Domain, you can use following options to filter</td>
<td>specific devices or device types:</td>
</tr>
<tr>
<td>specific devices or device types:</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Filters out devices containing a specified</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Filters out devices containing a specified</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Provides the sub-string to match. All devices</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Provides the sub-string to match. All devices</td>
<td></td>
</tr>
<tr>
<td>• exclude-controllers – Optional. Excludes all controllers in the specified RF</td>
<td></td>
</tr>
<tr>
<td>• exclude-controllers – Optional. Excludes all controllers in the specified RF</td>
<td></td>
</tr>
<tr>
<td>• exclude-controllers – Optional. Excludes all controllers in the specified RF</td>
<td></td>
</tr>
<tr>
<td>Domain from the reload process</td>
<td></td>
</tr>
<tr>
<td>• exclude-controllers – Optional. Excludes all controllers in the specified RF</td>
<td></td>
</tr>
<tr>
<td>Domain from the reload process</td>
<td></td>
</tr>
<tr>
<td>• filter &lt;DEVICE-TYPE&gt; – Optional. Filters devices by the device type specified.</td>
<td></td>
</tr>
<tr>
<td>• filter &lt;DEVICE-TYPE&gt; – Optional. Filters devices by the device type specified.</td>
<td></td>
</tr>
<tr>
<td>Select the type of device to reload. All devices, of the specified type, within</td>
<td></td>
</tr>
<tr>
<td>the specified RF Domain, are forcefully reloaded.</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-TYPE&gt; – Select the type of device to reload. The options are: AP621,</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-TYPE&gt; – Select the type of device to reload. The options are: AP621,</td>
<td></td>
</tr>
<tr>
<td>AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522,</td>
<td></td>
</tr>
<tr>
<td>AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500,</td>
<td></td>
</tr>
<tr>
<td>NX55XX, NX75XX, NX9000, VX9000, VX5200, VX9000, VX9000, VX9000. All devices of the type</td>
<td></td>
</tr>
<tr>
<td>specified are reloaded.</td>
<td></td>
</tr>
<tr>
<td>Note: If no device or RF Domain is specified, the system relogs the logged</td>
<td></td>
</tr>
<tr>
<td>device.</td>
<td></td>
</tr>
<tr>
<td>Initiates device(s) reloads and configures associated parameters</td>
<td></td>
</tr>
<tr>
<td>• staggered – Optional. Enables staggered reload of devices (one at a time)</td>
<td></td>
</tr>
<tr>
<td>• staggered – Optional. Enables staggered reload of devices (one at a time)</td>
<td></td>
</tr>
<tr>
<td>without network impact.</td>
<td></td>
</tr>
<tr>
<td>Use one of the following options to specify a single device, multiple devices, or</td>
<td></td>
</tr>
<tr>
<td>a RF Domain</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-MAC-OR-HOSTNAME&gt; – Optional. Performs staggered reload on specified</td>
<td></td>
</tr>
<tr>
<td>device(s) identified by the &lt;DEVICE-MAC-OR-HOSTNAME&gt; keyword. Specify the device’s</td>
<td></td>
</tr>
<tr>
<td>device’s hostname or MAC address. This is a recursive keyword that allows you to</td>
<td></td>
</tr>
<tr>
<td>specify multiple devices. When executed, the specified device(s) are halted and a</td>
<td></td>
</tr>
<tr>
<td>warm reboot is performed. Multiple devices are halted and rebooted one at a time</td>
<td></td>
</tr>
<tr>
<td>without impacting network functioning.</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-MAC-OR-HOSTNAME&gt; – Optional. Performs staggered reload of all devices</td>
<td></td>
</tr>
<tr>
<td>in a RF Domain. Specify the name of the RF Domain. When executed, devices in the</td>
<td></td>
</tr>
<tr>
<td>specified RF Domain are halted and rebooted one at a time without impacting</td>
<td></td>
</tr>
<tr>
<td>network functioning. Use additional filter options to filter devices in the specified</td>
<td></td>
</tr>
<tr>
<td>RF Domain.</td>
<td></td>
</tr>
<tr>
<td>Note: If no device or RF Domain is specified, the system relogs the logged</td>
<td></td>
</tr>
<tr>
<td>device.</td>
<td></td>
</tr>
<tr>
<td>When reloading devices in a RF Domain, you can use following options to filter</td>
<td>specific devices or device types:</td>
</tr>
<tr>
<td>specific devices or device types:</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Filters out devices containing a specified</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Filters out devices containing a specified</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Provides the sub-string to match. All devices</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;WORD&gt; – Optional. Provides the sub-string to match. All devices</td>
<td></td>
</tr>
<tr>
<td>• exclude-controllers – Optional. Excludes all controllers in the specified RF</td>
<td></td>
</tr>
<tr>
<td>Domain from the reload process</td>
<td></td>
</tr>
<tr>
<td>Contd..</td>
<td></td>
</tr>
</tbody>
</table>
Examples

rfs7000-6DCD4B#reload at 12:30:00 31 Mar 2015 on rfs6000-81742D
Reload scheduled at 2015-03-31 12:30:00 UTC ...
rfs7000-6DCD4B#

rfs7000-6DCD4B#reload cancel on rfs6000-81742D
Scheduled reload cancelled.
rfs7000-6DCD4B#

The following example schedules a reload on all non-controller devices in the RF Domain ‘default’:

rfs7000-6DCD4B#reload on default exclude-controllers
ap8132-711728: OK

rfs7000-6DCD4B#
3.1.47 rename

Privileged Exec Mode Commands

Renames a file in the devices' file system

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
rename <OLD-FILE-NAME> <NEW-FILE-NAME>

Parameters

- rename <OLD-FILE-NAME> <NEW-FILE-NAME>

Examples

rfs4000-229D58#dir
Directory of flash:/.

drwx Wed Jan 30 02:45:10 2014 log
drwx Sat Jan  1 00:00:09 2000 configs
drwx Sat Jan  1 00:00:08 2000 cache
drwx Wed Jan 16 22:26:53 2014 crashinfo
 drwx Fri Feb 15 14:50:49 2014 testdir
drwx Sat Jan  1 00:00:08 2000 upgrade
drwx Sat Jan  1 00:00:09 2000 hotspot
drwx Sat Jan  1 00:00:09 2000 floorplans
drwx Sat Jan  1 00:00:09 2000 startuplog
-rw- 176128 Fri Feb 15 14:32:51 2014 out.tar

rfs4000-229D58#

rfs4000-229D58#rename flash:/testdir/ Final
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

drwx Wed Jan 30 02:45:10 2014 log
drwx Sat Jan  1 00:00:09 2000 configs
drwx Fri Feb 15 14:50:49 2014 Final
drwx Sat Jan  1 00:00:08 2000 cache
drwx Fri Feb 15 14:50:49 2014 Final
drwx Wed Jan 16 22:26:53 2014 crashinfo
drwx Sat Jan  1 00:00:08 2000 upgrade
drwx Sat Jan  1 00:00:09 2000 hotspot
drwx Sat Jan  1 00:00:09 2000 floorplans
drwx Sat Jan  1 00:00:09 2000 startuplog
-rw- 176128 Fri Feb 15 14:32:51 2014 out.tar

rfs4000-229D58#
### 3.1.48 rmdir

**Privileged Exec Mode Commands**

Deletes an existing directory from the file system (only empty directories can be removed)

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext```
rmdir <DIR>
```

**Parameters**

- `rmdir <DIR>`

<table>
<thead>
<tr>
<th>rmdir &lt;DIR&gt;</th>
<th>Specifies the directory name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> The directory, specified by the &lt;DIR&gt; parameter, is removed from the file system.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58#dir
Directory of flash:/.

  drwx        Wed Jan 30  02:45:10 2014   log
  drwx        Sat Jan  1  00:00:09 2000   configs
  drwx        Fri Feb 15  14:50:49 2014   Final
  drwx        Sat Jan  1  00:00:08 2000   cache
  drwx        Wed Jan 16  22:26:53 2014   crashinfo
  drwx        Sat Jan  1  00:00:08 2000   upgrade
  drwx        Sat Jan  1  00:00:09 2000   hotspot
  drwx        Sat Jan  1  00:00:09 2000   floorplans
  drwx        Sat Jan  1  00:00:09 2000   startuplog
  -rw-       176128    Fri Feb 15  14:32:51 2014   out.tar

rfs4000-229D58#
```

```
rfs4000-229D58#rmdir Final
rfs4000-229D58#
```

```
rfs4000-229D58#dir
Directory of flash:/.

  drwx        Wed Jan 30  02:45:10 2014   log
  drwx        Sat Jan  1  00:00:09 2000   configs
  drwx        Sat Jan  1  00:00:08 2000   cache
  drwx        Wed Jan 16  22:26:53 2014   crashinfo
  drwx        Sat Jan  1  00:00:08 2000   upgrade
  drwx        Sat Jan  1  00:00:09 2000   hotspot
  drwx        Sat Jan  1  00:00:09 2000   floorplans
  drwx        Sat Jan  1  00:00:09 2000   startuplog
  -rw-       176128    Fri Feb 15  14:32:51 2014   out.tar

rfs4000-229D58#
```
3.1.49 **self**

Privileged Exec Mode Commands

Enters the logged device’s configuration context

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
self
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE#self
Enter configuration commands, one per line. End with CNTL/Z.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```
3.1.50 ssh

Privileged Exec Mode Commands

Opens a Secure Shell (SSH) connection between two network devices

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ssh <IP/HOSTNAME> <USERNAME> {<INF-NAME/LINK-LOCAL-ADD>}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Specify the remote system’s IP address or hostname.</td>
</tr>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify the name of the user requesting the SSH connection.</td>
</tr>
<tr>
<td>&lt;INF-NAME/\LINK-LOCAL-ADD&gt;</td>
<td>Optional. Specify the interface’s name or link local address.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To exit the other device’s context, use the command that is relevant to that device.

Examples

nx9500-6C8809#ssh 192.168.13.16 admin
admin@192.168.13.16's password:
rfs6000-6DB5D4>

nx9500-6C8809#ssh 192.168.13.14 admin
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.13.14' (RSA) to the list of known hosts. admin@192.168.13.14's password:
nx4500-5CFA8E>
Privileged Exec Mode Commands

Executes following operations on a T5 device through the WiNG controller:

- copy, rename, and delete files on the T5 device's file system
- write running configuration to the T5 device's memory

The T5 switch is a means of providing cost-effective, high-speed, wall-to-wall coverage across a building. The T5 switch leverages the in-building telephone lines to extend Ethernet and Wireless LAN networks without additional expenditure on re-wiring. This setup is ideally suited for hotels, providing high-speed Wi-Fi coverage to guest rooms.

The entire setup consists of the DSL T5 switch, TW-510 Ethernet wallplates, and TW-511 wireless wallplate access points. Replace the phone jack plate in a room with the TW-511 delivers 802.11 a/b/g/n and extend wireless connectivity in that room and the neighboring rooms. These TW-511 wallplates (also referred to as the CPEs) are connected to the T5 switch over the DSL interface using a phone block.

The T5 switch is adopted and managed through a WiNG controller. The connection between the T5 and WiNG switches is over a WebSocket.

### Syntax

```
t5 [copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>|delete <FILE-NAME>|rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>|write memory] {on <T5-DEVICE-NAME>}
```

### Parameters

- **t5** [copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>|delete <FILE-NAME>|rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>|write memory] {on <T5-DEVICE-NAME>}

<table>
<thead>
<tr>
<th><strong>copy</strong>&lt;br&gt;<strong>&lt;SOURCE-FILE-NAME&gt;</strong>&lt;br&gt;<strong>&lt;DEST-FILE-NAME&gt;</strong></th>
<th>Copies file to an external server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;SOURCE-FILE-NAME&gt;</code> – Specify the source file name.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEST-FILE-NAME&gt;</code> – Specify the destination file name.</td>
</tr>
<tr>
<td><strong>Note:</strong> The content from the source file is copied to the destination file.</td>
<td></td>
</tr>
<tr>
<td>The source or destination files can be local or remote FTP or TFTP files. The source file also can be a pre-defined keyword. At least one of the files should be a local file. Use this command to copy the startup and/or running configurations to an external server.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>delete</strong>&lt;br&gt;<strong>&lt;FILE-NAME&gt;</strong></th>
<th>Deletes files on the T5 device’s file system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;FILE-NAME&gt;</code> – Specify the file name. The specified file is deleted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>rename</strong>&lt;br&gt;<strong>&lt;SOURCE-FILE-NAME&gt;</strong>&lt;br&gt;<strong>&lt;DEST-FILE-NAME&gt;</strong></th>
<th>Renames a file on the T5 device’s file system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;SOURCE-FILE-NAME&gt;</code> – Specify the source file name</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEST-FILE-NAME&gt;</code> – Specify the new file name. The source file is renamed to the input provided here.</td>
</tr>
</tbody>
</table>

---

**NOTE:** For more information on other T5 CPE related commands, see cpe.
### write memory

Writes running configuration to an adopted T5 device's memory

- memory – Writes running configuration to the T5 device's *non-volatile* (NV) memory.

### on <T5-DEVICE-NAME>

Optional. Executes these operation on a specified T5 device

- `<T5-DEVICE-NAME>` – Specify the T5 device's hostname.

### Examples

```
rfa7000-37FABE#t5 write memory on t5-ED5C2C
Success
rfa7000-37FABE#
```
### 3.1.52 telnet

*Privileged Exec Mode Commands*

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}

**Parameters**

- telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Configures the remote system's IP (IPv4 or IPv6) address or hostname. The Telnet session will be established between the connecting system and the remote system.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP&gt; – Specify the remote system's IPv4 or IPv6 address or hostname.</td>
</tr>
<tr>
<td>&lt;INTF-NAME&gt;</td>
<td>Optional. Specify the interface name for the link local address.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To exit the other device’s context, use the command relevant to that device.

**Examples**

nx9500-6C8809#telnet 192.168.13.22

Entering character mode
Escape character is ‘[^]’.

AP7131 release 5.8.1.0-023D
ap7131-11B6C4 login: admin
Password: ap7131-11B6C4>
3.1.53 **terminal**

*Privileged Exec Mode Commands*

Sets the number of characters per line, and the number of lines displayed within the terminal window.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
terminal [length|width] <0-512>
```

**Parameters**

- `terminal [length|width] <0-512>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>Sets the number of lines displayed on the terminal window</td>
</tr>
<tr>
<td>width</td>
<td>Sets the width or number of characters displayed on the terminal window</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs7000-37FABE#terminal length 150</td>
<td></td>
</tr>
<tr>
<td>rfs7000-37FABE#terminal width 215</td>
<td></td>
</tr>
<tr>
<td>rfs7000-37FABE#show terminal</td>
<td>Terminal Type: xterm</td>
</tr>
<tr>
<td></td>
<td>Length: 150 Width: 215</td>
</tr>
</tbody>
</table>

**Related Commands**

```
no
```

Resets the width of the terminal window or the number of lines displayed on a terminal window.
3.1.54 **time-it**

> Privileged Exec Mode Commands

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

time-it <COMMAND>

**Parameters**

- time-it <COMMAND>

<table>
<thead>
<tr>
<th>time-it &lt;COMMAND&gt;</th>
<th>Verifies the time taken by a particular command to execute and provide a result</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;COMMAND&gt;</td>
<td>— Specify the command name.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE#time-it config terminal
Enter configuration commands, one per line. End with CNTL/Z.
That took 0.00 seconds..
rfs7000-37FABE(config)#
3.1.55 traceroute

> Privileged Exec Mode Commands

Traces the route to a defined destination

Use ‘--help’ or ‘-h’ to display a complete list of parameters for the traceroute command

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

traceroute <WORD>

Parameters

- traceroute <WORD>

<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Traces the route to a IP address or hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;WORD&gt; – Specify the IPv4 address or hostname.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809#traceroute 192.168.13.16
traceroute to 192.168.13.16 (192.168.13.16), 30 hops max, 46 byte packets
  1 192.168.13.16 (192.168.13.16) 0.479 ms 0.207 ms 0.199 ms
nx9500-6C8809#
3.1.56 traceroute6

Traces the route to a specified IPv6 destination

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
traceroute6 <WORD>

Parameters
- traceroute6 <WORD>

<table>
<thead>
<tr>
<th>traceroute6 &lt;WORD&gt;</th>
<th>Traces the route to a IPv6 address or hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>– Specify the IPv6 address or hostname.</td>
</tr>
</tbody>
</table>

Examples
rfs4000-1B3596# traceroute6 2001:10:10:10:10:10:10:2
  1  2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2) 0.622 ms 0.497 ms 0.531 ms
rfs4000-1B3596#
3.1.57 upgrade

Privileged Exec Mode Commands
Upgrades a device’s software image
Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
upgrade [<FILE>|<URL>|dhcp-vendor-options]
upgrade [<FILE>|<URL>]{background|on <DEVICE-NAME>}
upgrade dhcp-vendor-options {<DEVICE-NAME>|on <RF-DOMAIN-NAME>}
upgrade dhcp-vendor-options {<DEVICE-NAME>}{<DEVICE-NAME>}
upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>}{containing <SUB-STRING>|exclude-controllers|exclude-rf-domain-managers|filter <DEVICE-TYPE>}

Parameters
- upgrade [<FILE>|<URL>]{background|on <DEVICE-NAME>}

| <FILE> | Specify the target firmware image location in the following format:
|        | cf:/path/file
|        | usb1:/path/file
|        | usb2:/path/file
|        | usb<n>:/path/file
| <URL>  | Specify the target firmware image location. Use one of the following formats:
|        | IPv4 URLs:
|        | tftp://<hostname|IP>[:port]/path/file
|        | ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
|        | sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
|        | http://<hostname|IP>[:port]/path/file
|        | cf:/path/file
|        | usb<n>:/path/file
|        | IPv6 URLs:
|        | tftp://<hostname|IPv6>[:port]/path/file
|        | ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file
|        | sftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file
|        | http://<hostname|IPv6>[:port]/path/file

- background Optional. Performs upgrade in the background
- on <DEVICE-NAME> Optional. Upgrades the software image on a specified remote device
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
PRIVILEGED EXEC MODE COMMANDS 3-117

- upgrade dhcp-vendor-options {<DEVICE-NAME>} {<DEVICE-NAME>}

<table>
<thead>
<tr>
<th>dhcp-vendor-options</th>
<th>Uses DHCP vendor options to upgrade device(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>{&lt;DEVICE-NAME&gt;} {&lt;DEVICE-NAME&gt;}</td>
<td>Optional. Uses DHCP vendor options to upgrade a specified device. Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Optional. You can optionally specify multiple comma-separated device names/MAC addresses to upgrade.</td>
<td></td>
</tr>
</tbody>
</table>

- upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>} {containing <SUB-STRING>| exclude-controllers|exclude-rf-domain-managers|filter <DEVICE-TYPE>}

<table>
<thead>
<tr>
<th>dhcp-vendor-options</th>
<th>Uses DHCP vendor options to upgrade device(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;RF-DOMAIN-NAME&gt;</td>
<td>Optional. Uses DHCP vendor options to upgrade all devices or specified device(s) within the RF Domain identified by the &lt;RF-DOMAIN-NAME&gt; keyword</td>
</tr>
<tr>
<td>• &lt;RF-DOMAIN-NAME&gt; – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, all devices within the RF Domain are upgraded. These filters are:</td>
<td></td>
</tr>
<tr>
<td>• containing &lt;SUB-STRING&gt; – Optional. Upgrades all devices, within the specified RF Domain, containing a specified sub-string in their hostname</td>
<td></td>
</tr>
<tr>
<td>• &lt;SUB-STRING&gt; – Specify the sub-string to match.</td>
<td></td>
</tr>
<tr>
<td>• exclude-controllers – Optional. Upgrades all devices, within the specified RF Domain, excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.</td>
<td></td>
</tr>
<tr>
<td>• exclude-rf-domain-manager – Optional. Upgrades all devices, within the specified RF Domain, excluding RF Domain managers. Use this option when executing the command on the NOC, Site controller, or RF Domain manager.</td>
<td></td>
</tr>
<tr>
<td>• filter &lt;DEVICE-TYPE&gt; – Optional. Executes the command on all devices, within the specified RF Domain, of a specified type</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-TYPE&gt; – Specify the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, VX9000. Upgrades all devices of the type specified here. For example, if AP6521 is the device-type specified, all AP6521s within the specified RF Domain are upgraded.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE#show boot

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>BUILD DATE</th>
<th>INSTALL DATE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>03/05/2015 00:32:22</td>
<td>03/19/2015 22:46:12</td>
<td>5.8.1.0-023D</td>
</tr>
<tr>
<td>Secondary</td>
<td>03/03/2015 21:59:27</td>
<td>03/09/2015 00:15:31</td>
<td>5.8.1.0-021D</td>
</tr>
</tbody>
</table>

Current Boot : Primary
Next Boot : Primary
Software Fallback : Enabled
rfs7000-37FABE
rfs7000-37FABE# upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W58/RFS7000-024D.img
Running from partition /dev/mtdblock7
Validating image file header
Making file system
Extracting files (this may take some time)
..................................................................................
.......................................................................................
..................................
Control C disabled
Version of firmware update file is 5.8.1.0-024D
Removing unneeded files from flash:/crashinfo directory
Removing unneeded files from flash:/var2/log directory
FPGA firmware version is already at version 1_26, no need to upgrade
PoE updates are handled via a patch file
Power Supervisor updates are handled via a patch file
Checking if boot sector needs to be upgraded
Boot Sector version 00008, image file bootsector ver 00008, no change required
Writing Kernel to /dev/mtd4
Writing BootOS to /dev/mtd15
Successful
rfs7000-37FABE#

rfs7000-37FABE# show boot

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>BUILD DATE</th>
<th>INSTALL DATE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>03/05/2015</td>
<td>03/19/2015</td>
<td>5.8.1.0-023D</td>
</tr>
<tr>
<td>Secondary</td>
<td>03/20/2015</td>
<td>03/20/2015</td>
<td>5.8.1.0-024D</td>
</tr>
</tbody>
</table>

Current Boot : Primary
Next Boot : Secondary
Software Fallback : Enabled

After upgrading, the device has to be **reloaded** to boot using the new image.

The following example displays the devices adopted by the nx7500-7F3609 service platform:

nx7500-7F3609# show adoption status

<table>
<thead>
<tr>
<th>DEVICE-NAME</th>
<th>VERSION</th>
<th>CFG-STAT</th>
<th>MSGS ADOPTED-BY</th>
<th>LAST-ADOPTION</th>
<th>UPTIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs6000-18072B</td>
<td>5.8.1.0-007D</td>
<td>configured</td>
<td>No nx7500-7F3609</td>
<td>0 days 00:35:33</td>
<td>0 days 00:41:37</td>
</tr>
<tr>
<td>rfs7000-6DCBB3</td>
<td>5.8.0.0-042R</td>
<td>version-mismatch</td>
<td>No nx7500-7F3609</td>
<td>0 days 00:00:00</td>
<td>0 days 00:04:45</td>
</tr>
</tbody>
</table>

Total number of devices displayed: 2

nx7500-7F3609#

In the following example, only one device (rfs7000-6DCBB3) is being upgraded. The image file is located on a TFTP server. Path and file name are provided.

nx7500-7F3609# upgrade tftp://192.168.0.50/RFS7000-5.8.1.0-007D.img rfs7000-6DCBB3

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs7000-6DCBB3</td>
<td>Success</td>
<td>None</td>
</tr>
</tbody>
</table>

nx7500-7F3609# sh upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time : 2015-10-08 04:35:12

nx7500-7F3609#
The following example shows the upgrade status:

nx7500-7F3609#show upgrade detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2015-10-08 04:35:12
-----------------------------------------------
Running from partition /dev/sda7
var2 is 2 percent full
/tmp is 2 percent full
Free Memory 15258044 kB
FWU invoked via Linux shell
Validating image file header
Removing other partition
Making file system
Extracting files (this may take some time).
Control C disabled
Version of firmware update file is 5.8.1.0-007D
Creating LILO files
Running LILO
Successful

nx7500-7F3609#

nx7500-7F3609#show upgrade on rfs7000-6DCBB3
Last Image Upgrade Status : In_Progress(Establishing contact with server.)
Last Image Upgrade Time   : 2015-10-08 05:31:32
nx7500-7F3609#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes a patch installed on a specified device</td>
</tr>
</tbody>
</table>
3.1.58 **upgrade-abort**

- *Privileged Exec Mode Commands*

Aborts an ongoing software image upgrade

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrade-abort</td>
<td>Aborts an ongoing software image upgrade</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Aborts an ongoing software image upgrade on a specified device or domain</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W581/RFS4000.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time).................

rfs7000-37FABE#upgrade-abort on rfs4000-229D58
```

```
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W58/RFS4000.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time).................

*Update error: Aborted*
```

rfs4000-229D58#
3.1.59 watch

Privileged Exec Mode Commands
Repeats a specified CLI command at periodic intervals
Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
watch <1-3600> <LINE>

Parameters
- watch <1-3600> <LINE>

<table>
<thead>
<tr>
<th>watch &lt;1-3600&gt;</th>
<th>Repeats a CLI command at a specified interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3600&gt;</td>
<td>Select an interval from 1 - 3600 seconds. Pressing CTRL-Z halts execution of the command.</td>
</tr>
<tr>
<td>&lt;LINE&gt;</td>
<td>Specify the CLI command name.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE#watch 1 show clock
rfs7000-37FABE#
3.1.60 **exit**

*Privileged Exec Mode Commands*

Ends the current CLI session and closes the session window

For more information, see `exit`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9000, NX9500, NX9510, NX9600

**Syntax**

`exit`

**Parameters**

None

**Examples**

```
exit
```
3.1.61 smart-cache

Privileged Exec Mode Commands

Pre-fetches cached content from the specified list of URLs

Smart caching is a licensed service available on the NX45XX and NX65XX series service platforms. It allows the temporary storage of frequently accessed Web content (Web pages, graphics, audio and video files etc.) on network infrastructure devices. When this content is requested, it is retrieved from a local content cache and not from the origin server. For more information on enabling content caching, see smart-cache-policy.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX9000, NX9500, NX9510

Syntax

smart-cache pre-fetch-immediate <URL-LIST-NAME>

Parameters

- smart-cache pre-fetch-immediate <URL-LIST-NAME>

<table>
<thead>
<tr>
<th>smart-cache</th>
<th>Pre-fetches content from the specified list of URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-fetch-immediate &lt;URL-LIST-NAME&gt;</td>
<td>Provide the URL list names (should be existing and configured). For more information on configuring URL lists, see url-list.</td>
</tr>
</tbody>
</table>

Examples

nx4500-5CFA2B#smart-cache pre-fetch-immediate ?
  URL-LIST  URL List to be Pre Fetched

nx4500-5CFA2B#
3.1.62 virtual-machine

Privileged Exec Mode Commands

Installs, configures, and monitors the status of third-party virtual machines (VMs)

In addition to the WiNG VMs, the NX45XX, NX65XX, NX9500, and NX9510 series service platforms support the installation and administration of third-party VMs. However, the third-party VMs supported by these devices varies.

The third-party VMs supported on NX45XX and NX65XX are:

• TEAM-URC
• TEAM-RLS
• TEAM-VoWLAN

The VM supported on NX9500 and NX9510 is:

• ADSP

Use the virtual-machine command to install the third-party VMs, and configure parameters, such as install media type and location, number of Virtual Central Processing Units (VCPUS), VM memory, VM disk, number of Virtual Network Interfaces (VIFs), and Virtual Networking Computing (VNC) port.

Installing third-party VMs saves on hardware cost and provides a unified VM management interface.

This section is organized into the following sub-sections:

• Syntax NX45XX, NX65XX
• Syntax NX9500 and NX9510

Supported in the following platforms:

• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524,
  • NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax NX45XX, NX65XX

virtual-machine [assign-usb-ports|console|export|install|restart|set|start|stop|uninstall]

virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}

virtual-machine console [<VM-NAME>|team-urc|team-rls|team-vowlan]

virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}

virtual-machine install [<VM-NAME]|team-urc|team-rls|team-vowlan]

virtual-machine install <VM-NAME> type disk|iso disk-size <SIZE>|vm-archive
  install-media [<FILE>|<URL>|<USB>] {autostart|memory|on|vcpus|vif-count|vnc}

virtual-machine install [team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine restart [<VM-NAME]|hard|team-urc|team-rls|team-vowlan]

virtual-machine restart [on <DEVICE-NAME>]

virtual-machine restart hard [on <DEVICE-NAME>]

virtual-machine set [autostart|memory|vcpus|vif-count|vif-mac|vif-to-vmif|vnc]

virtual-machine set [on <DEVICE-NAME>]

virtual-machine start [auto-start ignore|start] [memory <512-8192>] [vcpus <1-4]|
  vif-count <0-2> [vif-mac <VIF-INDEX>] [vnc <DISABLE|ENABLE>] {on <DEVICE-NAME>}

virtual-machine start [on <DEVICE-NAME>]

virtual-machine stop [hard|team-urc|team-rls|team-vowlan]

virtual-machine stop [on <DEVICE-NAME>]

virtual-machine stop [on <DEVICE-NAME>]
virtual-machine stop hard [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine uninstall [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

Parameters NX45XX, NX65XX

• virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}

Assigns USB ports to TEAM-VoWLAN

• team-vowlan – Assigns USB ports to TEAM-VoWLAN on a specified device

• on <DEVICE-NAME> – Optional. Specify the device name.

Use the no > virtual-machine > assign-usb-ports command to reassign the port to WING.

Note: TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.

• virtual-machine console [<VM-NAME>|team-urc|team-rls|team-vowlan]

Connects to the VM’s console, based on the parameters passed. Select one of the following console options:

• <VM-NAME> – Connects to the console of the VM identified by the <VM-NAME> keyword. Specify the VM name.

• team-urc – Connects to the VM TEAM Unified Retail Communication’s (URC) (IP-PBX) console

• team-rls – Connects to the VM TEAM Radio Link Service (RLS) server’s console

• team-vowlan – Connects to the VM TEAM-VoWLAN’s (Voice over WLAN) console

• virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}

Exports an existing VM image and settings. Use this command to export the VM to another NX45XX or NX65XX device in the same domain.

• <VM-NAME> – Specify the VM name.

• <FILE> – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.

• <URL> – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path:

  tftp://<hostname|IP>[:port]/path/file

  ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

  sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

  http://<hostname|IP>[:port]/path/file

• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices.

• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

The VM should be in a stop state during the export process.

If the destination is a device, the image is copied to a predefined location (VM archive).

• virtual-machine install <VM-NAME> type [disk|iso disk-size <SIZE>|vm-archive] install-media [<FILE>|<URL>|<USB>] {autostart|memory|on|vcpus|vif-count|vnc}

Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process.

• <VM-NAME> – Specify the VM name.

• type – Specify the install-media (image) type. The options are:

  • disk – Specifies the install media type as pre-installed OS disk image (located in the flash memory) Contd..
• iso disk-size <SIZE> – Specifies the install media type as ISO file. This is a single file, which contains the OS bootable install media.
  • disk-size <SIZE> – If the install media type is ISO, specify the disk size in GB.
  • vm-archive – Specifies the install media type as VM archive. The VM archive file is a tar.gz file consisting of a pre-installed OS disk image and an associated configuration file. The configuration is a standard libvirt VM template consisting of VM specific information.

Note: After specifying the install media type, specify the location of the image. The image can be located in any of the following supported locations: FLASH, USB, or a remote location, such as http, ftp, sftp, tftp.

install-media
[<FILE>|<URL>|<USB>]
{autostart|memory|on|vcpus|vif-count|vnc}

Specifies the install media location
• <FILE> – Specifies the install-media file is located on flash, for example flash:/cache
• <URL> – Specifies the install-media file is located on a remote URL. Provide the URL using one of the following formats:
  tftp://<hostname|IP>[:<port>]/path/file
  ftp://<user>:<passwd>@<hostname|IP>[:<port>]/path/file
  sftp://<user>:<passwd>@<hostname|IP>[:<port>]/path/file
  http://<hostname|IP>[:<port>]/path/file
• <USB> – Specifies the install-media file is located on a USB. Provide the USB path and file name using the following format:
  usb<n>:/path/file

After specifying the image location, you may provide the following information:
• autostart – Optional. Specifies whether to autostart the VM on system reboot
  • ignore – Enables autostart on each system boot/reboot
  • start – Disables autostart (default setting)
• memory – Optional. Defines the VM memory size
  • <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 2048 MB.
• on – Optional. Executes the command on a specified device
  • <DEVICE-NAME> – Specify the service platform name.
• vcpus – Optional. Specifies the number of VCPUS for this VM
  • <1-4> – Specify the number of VCPUS from 1- 4. The default setting is 4.
• vif-count – Optional. Configures or resets the VIF number for this VM
  • <0-2> – Specify the VIF number from 0 - 2. the default setting is 1. If assigning a virtual network interface for the VM, optionally specify the following parameters:
    • vif-mac – Sets the MAC index for the virtual interfaces 1 & 2.
    • vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface.
      Specify the VMIF interface index from 1 - 8. VMIFs are layer 2 interfaces on the WiNG bridge. Each custom VM can have up to a maximum of 2 virtual Ethernet interfaces. By default, these interfaces are internally connected to the Dataplane bridge through VMIF1, which is an untagged port with access VLAN 1.
    • vnc – Enables VNC on the virtual interfaces 1 & 2
  • vnc – Optional. Disables/enables VNC port. When enabled, provides remote access to VGA through the noVNC client.
  • disable – Disables VNC
  • enable – Enables VNC (default setting)
• virtual-machine install [team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine install [team-urc|team-rls|team-vowlan]
on <DEVICE-NAME>
Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process. Select one of the following options:
• team-urc – Installs the VM TEAM-URC image
• team-rls – Installs the VM TEAM-RLS image
• team-vowlan – Installs the VM TEAM-VoWLAN image
The following keywords are common to all of the above parameters:
• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

• virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan]
{on <DEVICE-NAME>}

virtual-machine restart [<VM-NAME>|hard|team-urc|team-rls|team-vowlan]
Restarts the VM
• <VM-NAME> – Restarts the VM identified by the <VM-NAME> keyword
• team-urc – Restarts the VM TEAM-URC
• team-rls – Restarts the VM TEAM-RLS
• team-vowlan – Restarts the VM TEAM-VoWLAN
The following keywords are common to all of the above parameters:
• on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
• <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
The option 'hard' forces the specified VM to restart.

• virtual-machine set [autostart [ignore|start]|memory <512-8192>|vcpus <1-4>
vif-count <0-2>|vif-mac <VIF-INDEX> [MAC-INDEX]|MAC|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>|vnc [disable|enable]] [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine set autostart [ignore|start]
memory <512-8192>vcpus <1-4>vif-count <0-2>vif-mac <VIF-INDEX> [MAC-INDEX]|MAC|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>vnc [disable|enable]
[<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
Configures the VM settings
• autostart – Specifies whether to autostart the VM on system reboot
  • ignore – Enables autostart on each system reboot
  • start – Disables autostart
• memory – Defines the VM memory size
  • <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.
• vcpus – Specifies the number of VCPUS for this VM
  • <1-4> – Specify the number of VCPUS from 1- 4.
• vif-count – Configures or resets the VM’s VIFs
  • <0-2> – Specify the Virtual Interface (VIF) number from 0 - 2.
• vif-mac – Configures the MAC address of the selected virtual network interface
  • <VIF-INDEX> – Select the VIF Index from 1 - 2.
  • <MAC-INDEX> – Specify the MAC index for the selected VIF from 1 - 8.
  • <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.

Contd..
Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the ‘set’ keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard l2 ports on the DP bridge, supporting all VLAN and ACL commands. The WiNG software supports up to a maximum of 8 VMIFs. By default, a VM’s interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the `vif-to-vmif` command to map a VIF to a VMIF on the DP bridge.

- `vif-to-vmif` – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.
  - `<VIF-INDEX>` – Selects the VIF index from 1 - 2.
  - `<VMIF-INDEX>` – Specify the VMIF index from 1 - 8.

WiNG provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of the eight VMIF ports for NX4500 and NX6500 service platforms and twelve ports for NX9500 on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.

- `vnc` – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.
  - `disable` – Disables VNC port
  - `enable` – Enables VNC port

After configuring the VM settings, identify the VM to apply the settings.

- `<VM-NAME>` – Applies these settings to the VM identified by the `<VM-NAME>` keyword. Specify the VM name.
- `team-urc` – Applies these settings to the VM TEAM-URC
- `team-rls` – Applies these settings to the VM TEAM-RLS
- `team-vowlan` – Applies these settings to the VM TEAM-VoWLAN
  - on `<DEVICE-NAME>` – Optional. Executes the command on a specified device or devices
  - `<DEVICE-NAME>` – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

- **virtual-machine start** `[<VM-NAME>][team-urc|team-rls|team-vowlan] [on `<DEVICE-NAME>`]`
The following keywords are common to all of the above parameters:
- **on <DEVICE-NAME>** – Optional. Executes the command on a specified device or devices
- **<DEVICE-NAME>** – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**virtual-machine stop**

```
virtual-machine stop [<VM-NAME>|hard|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

Stops the VM, based on the parameters passed. Select one of the following options:
- **<VM-NAME>** – Stops the VM identified by the **<VM-NAME>** keyword. Specify the VM name.
- **team-urc** – Stops the VM TEAM-URC
- **team-rls** – Stops the VM TEAM-RLS
- **team-vowlan** – Stops the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:
- **on <DEVICE-NAME>** – Optional. Executes the command on a specified device or devices
- **<DEVICE-NAME>** – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

The option 'hard' forces the selected VM to shutdown.

**virtual-machine uninstall**

```
virtual-machine uninstall [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

Uninstalls the specified VM
- **<VM-NAME>** – Uninstalls the VM identified by the **<VM-NAME>** keyword. Specify the VM name.
- **team-urc** – Uninstalls the VM TEAM-URC
- **team-rls** – Uninstalls the VM TEAM-RLS
- **team-vowlan** – Uninstalls the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:
- **on <DEVICE-NAME>** – Optional. Executes the command on a specified device or devices
- **<DEVICE-NAME>** – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**Note:** This command releases the VM’s resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system.

**Syntax NX9500 and NX9510**

```
virtual-machine

virtual-machine console adsp
virtual-machine install [adsp] {on <DEVICE-NAME>}
virtual-machine restart [adsp] {on <DEVICE-NAME>}
virtual-machine set disk-size <100-500> adsp {on <DEVICE-NAME>}
virtual-machine set memory <512-8192> adsp {on <DEVICE-NAME>}
virtual-machine set wing-memory <12288-32739>
virtual-machine [start|stop] adsp {on <DEVICE-NAME>}
virtual-machine uninstall adsp {on <DEVICE-NAME>}
```

**NOTE:** On an NX95XX, you can use the install, start, stop, restart, and set commands to manage a third-party VM running on a NX45XX and NX65XX. You can also configure a third-party VM’s settings through a NX95XX series service platform.
### Parameters NX9500 and NX9510

- **virtual-machine console adsp**

  Connects to the *Air-Defense Services Platform* (ADSP) VM's management console. When ADSP is running on the NX9500 and NX9510 model service platforms, WiNG communicates with ADSP using a *single sign-on* (SSO) authentication mechanism. Once the user is logged in, WiNG gains access to ADSP without being prompted to login again at ADSP. However, the WiNG and ADSP databases are not synchronized. ADSP has its own user database, stored locally within its VM, which is accessed whenever a user logs directly into ADSP.

  WiNG and ADSP must be consistent in the manner events are reported up through a network hierarchy to ensure optimal interoperability and event reporting. To provide such consistency, WiNG has added support for an ADSP-like hierarchal tree. The tree resides within WiNG, and ADSP reads it from WiNG and displays the network hierarchy in its own ADSP interface. The hierarchal tree can also be used to launch ADSP modules (like Spectrum Analyzer) directly from WiNG. For more information on configuring WiNG tree-node structure, see [tree-node](#).

- **virtual-machine install adsp {on <DEVICE-NAME>]**

  Installs the ADSP VM
  - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

  Before installing the ADSP VM, execute the upgrade command, giving the path and file name of the ADSP firmware image. This extracts the image on to the device (NX9500 or NX9510) on which the command has been executed. On successful completion of this process, execute the reload command to reboot the device. Once the device has been successfully rebooted, execute the `virtual-machine > install > adsp` command.

  For example:

  ```plaintext
  #upgrade tftp://20.1.1.60/adsp-9.1.1May 29 15:12:41 2015: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 192 "-" "-
  03-5.8.1.0-008D.img
  May 29 15:12:51 2014: nx9500-6C874D : %DIAG-6-
  NEW_LED_STATE: LED state message FIRMWARE_UPGRADE_STARTED
  from module led_msg
  Running from partition /dev/sda8
  Validating image file header
  Extracting files (this may take some time).....May 29 15:12:53 2014: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 923 "-" "-
  ...........
  ```

- **virtual-machine restart adsp {on <DEVICE-NAME>]**

  Restarts the ADSP VM
  - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| virtual-machine set disk-size <100-500> adsp {on <DEVICE-NAME>} | Sets the ADSP VM's disk size (in GB)  
  - <100-500> – Specify a value from 100 - 500 GB.  
  - adsp – Sets the VM as ADSP  
    - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices  
    - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.  
  Stop the ADSP VM before executing this command. |
| virtual-machine set memory <512-8192> adsp {on <DEVICE-NAME>} | Modifies the ADSP VM's memory  
  - <512-8192> – Specify a value from 512 - 8192 MB.  
  - adsp – Sets the VM as ADSP  
    - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices  
    - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |
| virtual-machine set wing-memory <12288-32739> | Specifies the WiNG memory size in MB  
  This command is applicable only to the NX9500 and NX9510 service platforms. Use the `show > virtual-machine-configuration` command to view the configured memory allocation. Use the `show > virtual-machine-statistics` to view the current allocated memory allocation.  
  - <12288-32739> – Specify a value from 12288 - 32739 MB. The default is 18432 MB.  
  The new memory setting takes effect only after the next boot. |
| virtual-machine [start|stop] adsp {on <DEVICE-NAME>} | Starts/stops the ADSP VM  
  - start – Starts the ADSP VM. Use this command to boot a shut down VM (in a stop state).  
  - stop – Stops a running ADSP VM. Use this command to shut down a running VM.  
    - on <DEVICE-NAME> – Optional. Executes the start/stop command on a specified device or devices  
    - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |
| virtual-machine uninstall adsp {on <DEVICE-NAME>} | Uninstalls the ADSP VM  
  - adsp – Sets the VM as ADSP  
    - on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices  
    - <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas. |
Examples
The following examples show the VM installation process:

Installation media: USB

<DEVICE>#virtual-machine install <VM-NAME> type iso disk-size 8 install-media usb1://vms/win7.iso autostart start memory 512 vcpus 3 vif-count 2 vnc enable

Installation media: pre-installed disk image

<DEVICE>##virtual-machine install <VM-NAME> type disk install-media flash:/vms/win7_disk.img autostart start memory 512 vcpus 3 vif-count 2 vnc-enable on <DEVICE-NAME>

In the preceding example, the command is executed on the device identified by the <DEVICE-NAME> keyword. In such a scenario, the disk-size is ignored if specified. The VM has the install media as first boot device.

Installation media: VM archive

<DEVICE>#virtual-machine install type vm-archive install-media flash:/vms/<VM-NAME> vcpus 3

In the preceding example, the default configuration attached with the VM archive overrides any parameters specified.

Exporting an installed VM:

<DEVICE>#virtual-machine export <VM-NAME> <URL> on <DEVICE-NAME>

In the preceding example, the command copies the VM archive on to the URL (VM should be in stop state).

nx4500-5CFA2B#virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
nx4500-5CFA2B#

**NOTE:** Use the `show > virtual-machine` command to view installed VM details.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reassigns USB port to WiNG</td>
</tr>
</tbody>
</table>
3.1.63 raid

Privileged Exec Mode Commands

Enables Redundant Array of Independent Disks (RAID) management

RAID is a group of one or more independent, physical drives, referred to as an array or drive group. These physically independent drives are linked together and appear as a single storage unit or multiple virtual drives. Replacing a single, large drive system with an array, improves performance (input and output processes are faster) and increases fault tolerance within the data storage system.

In an array, the drives can be organized in different ways, resulting in different RAID types. Each RAID type is identified by a number, which determines the RAID level. The common RAID levels are 0, 00, 1, 5, 6, 50 and 60. The WiNG MegaRAID implementation supports RAID-1, which provides data mirroring, but does not support data parity. RAID-1 consists of a two-drive array, where the data is simultaneously written on both drives, ensuring total data redundancy. In case of a drive failure the information on the other drive is used to rebuild the failed drive.

An array is said to be degraded when one of its drives has failed. A degraded array continues to function and can be rebooted using the one remaining functional drive. When a drive fails, the chassis sounds an alarm (if enabled), and the CLI prompt changes to "RAID degraded". The failed drive is automatically replaced with a hot spare (provided a spare is installed). The spare is used to re-build the array.

Use this command to:

• Verify the current array status
• Start and monitor array consistency checks
• Retrieve date and time of the last consistency check
• Shut down drives before physically removing them
• Install new drives
• Assign drives as hot spares
• Identify a degraded drive
• Deactivate an alarm (triggered when a drive is removed from the array)

Supported in the following platforms:
• Service Platforms — NX7530, NX9500

Syntax
raid [check|install|locate|remove|silence|spare]
raid [check|silence]
raid [install|locate|remove|spare] drive <0-4>

Parameters
• raid [check|silence]

| check | Starts a consistency check on the RAID array. Use the show > raid command to view consistency check status. A consistency check verifies the data stored in the array. When regularly executed, it helps protect against data corruption, and ensures data redundancy. Consistency checks also warn of potential disk failures. |
### raid [install|locate|remove|spare] drive <0-4>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| silence  | Deactivates an alarm | **Note:** When enabled, an audible alarm is triggered when a drive in the array fails. The *silence* command deactivates the alarm (sound). **Note:** To enable RAID alarm, in the device configuration mode, use the *raid > alarm > enable* command. A NX9500 profile can also have the RAID alarm feature activated. For more information on the enabling RAID alarm, see *raid*.

### Examples

```
nx9500-6C874D#raid install drive 0
Error: Input Error: Drive 0 is already member of array, can't be added
nx9500-6C874D#  
```
CHAPTER 4
GLOBAL CONFIGURATION COMMANDS

This chapter summarizes the global-configuration commands in the CLI command structure.

The term global indicates characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The following example describes the process of entering the global configuration mode from the PRIV EXEC mode:

<DEVICE>#configure terminal
<DEVICE>(config)#

NOTE: The system prompt changes to indicate you are now in the global configuration mode. The prompt consists of the device host name followed by (config) and a pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a commit write memory command is issued.

<DEVICE>(config)#?
Global configuration commands:
  aaa-policy
    Configure a authentication/accounting/authorization policy
  aaa-tacacs-policy
    Configure an authentication/accounting/authorization TACACS policy
  alias
    Alias
  ap621
    AP621 access point
  ap622
    AP622 access point
  ap650
    AP650 access point
  ap6511
    AP6511 access point
  ap6521
    AP6521 access point
  ap6522
    AP6522 access point
  ap6532
    AP6532 access point
  ap6562
    AP6562 access point
  ap71xx
    AP71XX access point
  ap7502
    AP7502 access point
  ap7522
    AP7522 access point
  ap7532
    AP7532 access point
  ap7562
    AP7562 access point
  ap81xx
    AP81XX access point
ap82xx                              AP82XX access point
application                         Configure an application
application-policy                  Configure an application policy
association-acl-policy              Configure an association acl policy
auto-provisioning-policy            Configure an auto-provisioning policy
bgp                                 BGP Configuration
bonjour-gw-discovery-policy         Bonjour Gateway discovery policy
bonjour-gw-forwarding-policy        Bonjour Gateway forwarding policy
bonjour-gw-query-forwarding-policy  Bonjour Gateway Query forwarding policy
captive-portal                      Configure a captive portal
clear                               Clear
client-identity                     Client identity (DHCP Device Fingerprinting)
client-identity-group               Client identity group (DHCP Fingerprint Database)
clone                               Clone configuration object
crypto-cmp-policy                   CMP policy
customize                           Customize the output of summary cli commands
device                              Configuration on multiple devices
device-categorization               Configure a device categorization object
dhcp-server-policy                  DHCP server policy
dhcpv6-server-policy                DHCPv6 server related configuration
dns-whitelist                       Configure a whitelist
event-system-policy                 Configure a event system policy
ex3500                              EX3500 device
ex3500-management-policy            Configure a ex3500 management policy
ex3500-qos-class-map-policy         Configure a ex3500 qos class-map policy
ex3500-qos-policy-map               Configure a ex3500 qos policy-map
ex3524                              EX3524 wireless controller
ex3548                              EX3548 wireless controller
firewall-policy                     Configure firewall policy
global-association-list            Configure a global association list
guest-management                   Configure a guest management policy
help                                Description of the interactive help system
host                                Enter the configuration context of a device by specifying its hostname
igmp-snoop-policy                   Create igmp snoop policy
inline-password-encryption         Store encryption key in the startup configuration file
ip                                  Internet Protocol (IP)
ipv6                                Internet Protocol version 6 (IPv6)
ipv6-router-advertisement-policy   IPv6 Router Advertisement related configuration
l2tpv3                              L2tpv3 tunnel protocol
mac                                 MAC configuration
management-policy                   Configure a management policy
meshpoint                           Configure a meshpoint quality-of-service policy
mint-policy                         Configure the global mint policy
nac-list                            Configure a network access control list
no                                  Configure a Nsight policy
nx45xx                              NX45XX integrated services platform
nx5500                              NX5500 wireless controller
nx65xx                              NX65XX integrated services platform
nx75xx                              NX75XX wireless controller
nx9000                              NXX9000 wireless controller
passpoint-policy                    Configure a passpoint policy
password-encryption                 Encrypt passwords in configuration
profile                             Profile related commands - if no parameters are given, all profiles are selected
radio-qos-policy                    Configure a radio quality-of-service policy
radius-group                         Configure radius user group parameters
radius-server-policy
radius-user-pool-policy
rename
rf-domain
rfs4000
rfs6000
rfs7000
roaming-assist-policy
role-policy
route-map
routing-policy
self
smart-cache-policy
smart-rf-policy
t5
url-filter
url-list
vx9000
web-filter-policy
wips-policy
wlan
wlan-qos-policy
write
c1rscrb
commit
do
end
exit
revert
service
show
</DEVICE>(config)#
## 4.1 Global Configuration Commands

### GLOBAL CONFIGURATION COMMANDS

The following table summarizes Global Configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-policy</td>
<td>Configures a AAA policy</td>
<td>page 4-9</td>
</tr>
<tr>
<td>aaa-tacacs-policy</td>
<td>Configures AAA-TACACS policy</td>
<td>page 4-17</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, VLAN, and service aliases</td>
<td>page 4-10</td>
</tr>
<tr>
<td>ap621</td>
<td>Adds an AP621 to the network</td>
<td>page 4-18</td>
</tr>
<tr>
<td>ap622</td>
<td>Adds an AP622 to the network</td>
<td>page 4-19</td>
</tr>
<tr>
<td>ap650</td>
<td>Adds an AP650 to the network</td>
<td>page 4-20</td>
</tr>
<tr>
<td>ap6511</td>
<td>Adds an AP6511 to the network</td>
<td>page 4-21</td>
</tr>
<tr>
<td>ap6521</td>
<td>Adds an AP6521 to the network</td>
<td>page 4-22</td>
</tr>
<tr>
<td>ap6522</td>
<td>Adds an AP6522 to the network</td>
<td>page 4-23</td>
</tr>
<tr>
<td>ap6532</td>
<td>Adds an AP6532 to the network</td>
<td>page 4-24</td>
</tr>
<tr>
<td>ap6562</td>
<td>Adds an AP6562 to the network</td>
<td>page 4-25</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Adds an AP71XX to the network</td>
<td>page 4-26</td>
</tr>
<tr>
<td>ap7502</td>
<td>Adds an AP7502 to the network</td>
<td>page 4-27</td>
</tr>
<tr>
<td>ap7522</td>
<td>Adds an AP7522 to the network</td>
<td>page 4-28</td>
</tr>
<tr>
<td>ap7532</td>
<td>Adds an AP7532 to the network</td>
<td>page 4-29</td>
</tr>
<tr>
<td>ap7562</td>
<td>Adds an AP7562 to the network</td>
<td>page 4-30</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Adds an AP81XX to the network</td>
<td>page 4-31</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Adds an AP82XX to the network</td>
<td>page 4-32</td>
</tr>
<tr>
<td>application</td>
<td>Creates an application definition and enters its configuration mode.</td>
<td>page 4-33</td>
</tr>
<tr>
<td>application-policy</td>
<td>Creates an application policy and enters its configuration mode</td>
<td>page 4-42</td>
</tr>
<tr>
<td>association-acl-policy</td>
<td>Configures an association ACL policy</td>
<td>page 4-59</td>
</tr>
<tr>
<td>auto-provisioning-policy</td>
<td>Configures an auto provisioning policy, which defines the process by which an access point discovers controllers and associates with it.</td>
<td>page 4-60</td>
</tr>
<tr>
<td>bgp</td>
<td>Configures Border Gateway Protocol (BGP) settings</td>
<td>page 4-61</td>
</tr>
<tr>
<td>bonjour-gw-discovery-policy</td>
<td>Configures a Bonjour GW Discovery policy (RFS7000 and AP7131)</td>
<td>page 4-63</td>
</tr>
<tr>
<td>bonjour-gw-forwarding-policy</td>
<td>Configures a Bonjour GW Forwarding policy (RFS7000 and AP7131)</td>
<td>page 4-65</td>
</tr>
</tbody>
</table>
### Table 4.1 Global Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bonjour-gw-query-forwarding-policy</code></td>
<td>Configures a Bonjour GW Query Forwarding policy, which enables Bonjour query forwarding across multiple VLANs (RFS7000 and AP7131)</td>
<td>page 4-66</td>
</tr>
<tr>
<td><code>captive portal</code></td>
<td>Configures a captive portal</td>
<td>page 4-67</td>
</tr>
<tr>
<td><code>clear</code></td>
<td>Clears the event history</td>
<td>page 4-107</td>
</tr>
<tr>
<td><code>client-identity</code></td>
<td>Enables client identification through DHCP device fingerprinting</td>
<td>page 4-108</td>
</tr>
<tr>
<td><code>client-identity-group</code></td>
<td>Creates a new client identity group and enters its configuration mode</td>
<td>page 4-116</td>
</tr>
<tr>
<td><code>clone</code></td>
<td>Clones a specified configuration object</td>
<td>page 4-123</td>
</tr>
<tr>
<td><code>crypto-cmp-policy</code></td>
<td>Creates a crypto Certificate Management Protocol (CMP) policy and enters its configuration mode</td>
<td>page 4-124</td>
</tr>
<tr>
<td><code>customize</code></td>
<td>Customizes the CLI command summary output</td>
<td>page 4-125</td>
</tr>
<tr>
<td><code>device</code></td>
<td>Specifies configuration on multiple devices</td>
<td>page 4-136</td>
</tr>
<tr>
<td><code>device-categorization</code></td>
<td>Configures a device categorization object</td>
<td>page 4-138</td>
</tr>
<tr>
<td><code>dhcp-server-policy</code></td>
<td>Configures a DHCP server policy</td>
<td>page 4-143</td>
</tr>
<tr>
<td><code>dhcpv6-server-policy</code></td>
<td>Configures DHCPv6 server policy parameters, such as class, address range, and options</td>
<td>page 4-144</td>
</tr>
<tr>
<td><code>dns-whitelist</code></td>
<td>Configures a DNS whitelist</td>
<td>page 4-146</td>
</tr>
<tr>
<td><code>event-system-policy</code></td>
<td>Configures an event system policy</td>
<td>page 4-152</td>
</tr>
<tr>
<td><code>ex3500</code></td>
<td>Creates an EX3500 time range list and enters its configuration mode</td>
<td>page 4-168</td>
</tr>
<tr>
<td><code>ex3500-management-policy</code></td>
<td>Creates an EX3500 management policy and enters its configuration mode</td>
<td>page 4-174</td>
</tr>
<tr>
<td><code>ex3500-qos-class-map-policy</code></td>
<td>Creates an EX3500 QoS class map policy and enters its configuration mode</td>
<td>page 4-192</td>
</tr>
<tr>
<td><code>ex3500-qos-policy-map</code></td>
<td>Creates an EX3500 QoS policy map and enters its configuration mode</td>
<td>page 4-200</td>
</tr>
<tr>
<td><code>ex3524</code></td>
<td>Adds a EX3524 switch to the network</td>
<td>page 4-214</td>
</tr>
<tr>
<td><code>ex3548</code></td>
<td>Adds a EX3548 switch to the network</td>
<td>page 4-216</td>
</tr>
<tr>
<td><code>firewall-policy</code></td>
<td>Configures a firewall policy</td>
<td>page 4-217</td>
</tr>
<tr>
<td><code>global-association-list</code></td>
<td>Configures a global list of client MAC addresses</td>
<td>page 4-219</td>
</tr>
<tr>
<td><code>guest-management</code></td>
<td>Configures a guest management policy that redirects guest users to a registration portal, upon association to a captive portal Service Set Identifier (SSID)</td>
<td>page 4-222</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>host</td>
<td>Sets the system's network name</td>
<td>page 4-232</td>
</tr>
<tr>
<td>inline-password-encryption</td>
<td>Stores the encryption key in the startup configuration file</td>
<td>page 4-233</td>
</tr>
<tr>
<td>ip</td>
<td>Creates a IP access control list (ACL) and/or a Simple Network Management Protocol (SNMP) ACL, and enters its configuration mode</td>
<td>page 4-234</td>
</tr>
<tr>
<td>ipv6</td>
<td>Creates a IPv6 ACL and enters its configuration mode</td>
<td>page 4-236</td>
</tr>
<tr>
<td>ipv6-router-advertisement-policy</td>
<td>Creates an IPv6 router advertisement (RA) policy and enters its configuration mode</td>
<td>page 4-237</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Configures Layer 2 Tunneling Protocol Version 3 (L2TPV3) tunnel policy</td>
<td>page 4-255</td>
</tr>
<tr>
<td>mac</td>
<td>Configures MAC access lists (goes to the MAC ACL mode)</td>
<td>page 4-257</td>
</tr>
<tr>
<td>management-policy</td>
<td>Configures a management policy</td>
<td>page 4-258</td>
</tr>
<tr>
<td>meshpoint</td>
<td>Configures meshpoint related configuration commands</td>
<td>page 4-260</td>
</tr>
<tr>
<td>meshpoint-qos-policy</td>
<td>Configures a set of parameters that defines the quality of service (QoS)</td>
<td>page 4-262</td>
</tr>
<tr>
<td>mint-policy</td>
<td>Configures a MiNT security policy</td>
<td>page 4-263</td>
</tr>
<tr>
<td>nac-list</td>
<td>Configures a network ACL</td>
<td>page 4-264</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 4-270</td>
</tr>
<tr>
<td>nsight-policy</td>
<td>Creates an NSight policy and enters its configuration mode</td>
<td>page 4-274</td>
</tr>
<tr>
<td>passpoint-policy</td>
<td>Creates a new passpoint policy and enters its configuration mode</td>
<td>page 4-283</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Enables password encryption</td>
<td>page 4-285</td>
</tr>
<tr>
<td>profile</td>
<td>Configures profile related commands</td>
<td>page 4-286</td>
</tr>
<tr>
<td>radio-qos-policy</td>
<td>Configures a radio qos policy</td>
<td>page 4-290</td>
</tr>
<tr>
<td>radius-group</td>
<td>Configures a RADIUS group</td>
<td>page 4-291</td>
</tr>
<tr>
<td>radius-server-policy</td>
<td>Configures a RADIUS server policy</td>
<td>page 4-292</td>
</tr>
<tr>
<td>radius-user-pool-policy</td>
<td>Configures a RADIUS user pool policy</td>
<td>page 4-293</td>
</tr>
<tr>
<td>rename</td>
<td>Renames and existing top-level object (TLO)</td>
<td>page 4-294</td>
</tr>
<tr>
<td>rf-domain</td>
<td>Creates an RF Domain</td>
<td>page 4-298</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Adds an RFS4000 to the network</td>
<td>page 4-329</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Adds an RFS6000 to the network</td>
<td>page 4-330</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Adds an RFS7000 to the network</td>
<td>page 4-331</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Adds an NX45XX to the network</td>
<td>page 4-332</td>
</tr>
<tr>
<td>nx5500</td>
<td>Adds an NX5500 to the network</td>
<td>page 4-333</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Adds an NX65XX to the network</td>
<td>page 4-334</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Adds an NX75XX to the network</td>
<td>page 4-335</td>
</tr>
<tr>
<td>nx9000</td>
<td>Adds a NX9000, NX9500, or NX9510 to the network</td>
<td>page 4-336</td>
</tr>
<tr>
<td>roaming-assist-policy</td>
<td>Configures a roaming assist policy that enables access points to assist wireless clients in making roaming decisions, such as which access point to connect etc.</td>
<td>page 4-337</td>
</tr>
<tr>
<td>role-policy</td>
<td>Configures a role policy</td>
<td>page 4-338</td>
</tr>
<tr>
<td>route-map</td>
<td>Creates a dynamic BGP route map and enters its configuration mode</td>
<td>page 4-339</td>
</tr>
<tr>
<td>routing-policy</td>
<td>Configures a routing policy</td>
<td>page 4-340</td>
</tr>
<tr>
<td>self</td>
<td>Displays a logged device’s configuration context</td>
<td>page 4-341</td>
</tr>
<tr>
<td>smart-rf-policy</td>
<td>Configures a Smart RF policy</td>
<td>page 4-342</td>
</tr>
<tr>
<td>t5</td>
<td>Configures a t5 wireless controller. This command is applicable only on the RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600 platforms.</td>
<td>page 4-343</td>
</tr>
<tr>
<td>web-filter-policy</td>
<td>Creates a Web Filtering policy and enters its configuration mode</td>
<td>page 4-345</td>
</tr>
<tr>
<td>wips-policy</td>
<td>Configures a WIPS policy</td>
<td>page 4-355</td>
</tr>
<tr>
<td>wlan</td>
<td>Configures a wireless WLAN</td>
<td>page 4-357</td>
</tr>
<tr>
<td>wlan-qos-policy</td>
<td>Configures a WLAN QoS policy</td>
<td>page 4-447</td>
</tr>
<tr>
<td>smart-cache-policy</td>
<td>Enables content caching to allow temporary storing of frequently accessed content on an intermediate network device. This command is specific to the NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, and NX9600 series service platforms.</td>
<td>page 4-449</td>
</tr>
<tr>
<td>url-filter</td>
<td>Creates a new URL filter and enters its configuration mode. URL filtering is a licensed feature.</td>
<td>page 4-467</td>
</tr>
<tr>
<td>url-list</td>
<td>Creates an URL list. This command is specific to the NX4500, NX4524, NX6500, and NX6524 series service platforms.</td>
<td>page 4-481</td>
</tr>
<tr>
<td>vx9000</td>
<td>Configures a Virtual WLAN Controller (V-WLC) in a virtual machine (VM) environment</td>
<td>page 4-486</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
NOTE: The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character.
4.1.1  aaa-policy

Configures an Authentication, Accounting, and Authorization (AAA) policy. This policy configures multiple servers for authentication and authorization. Up to six servers can be configured for providing AAA services.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
aaa-policy <AAA-POLICY-NAME>
```

Parameters

- `aaa-policy <AAA-POLICY-NAME>`

Examples

```
rfs7000-37FABE(config)#aaa-policy test
rfs7000-37FABE(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting        Configure accounting parameters
  attribute         Configure RADIUS attributes in access and accounting requests
  authentication    Configure authentication parameters
  health-check      Configure server health-check parameters
  mac-address-format Configure the format in which the MAC address must be filled in the Radius-Request frames
  no                 Negate a command or set its defaults
  proxy-attribute   Configure radius attribute behavior when proxying through controller or rf-domain-manager
  server-pooling-mode Configure the method of selecting a server from the pool of configured AAA servers
  use                Set setting to use
  clrscr             Clears the display screen
  commit             Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert             Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal
```

Related Commands

- `no`  Removes an existing AAA policy

NOTE: For more information on the AAA policy commands, see Chapter 8, AAA-POLICY.
4.1.2 alias

4.1.2.1 Global Configuration Commands

Configures network, VLAN, host, string, and network-service aliases

Aliases are objects having a unique name and content that is determined by the alias type (network, VLAN, and network-service).

A typical large enterprise network consists of multiple sites (RF Domains) having similar configuration parameters with few elements that vary, such as networks or network ranges, hosts having different IP addresses, and VLAN IDs or URLs. These elements can be defined as aliases (object oriented wireless firewalls) and used across sites by applying overrides to the object definition. Using aliases results in a configuration that is easier to understand and maintain.

Multiple instances of an alias (same type and same name) can be defined at any of the following levels: global, RF Domain, profile, or device. An alias defined globally functions as a top-level-object (TLO). Global aliases are not mandatory, and can be defined at the domain-level, or profile, or device-level only. An alias defined on a device is applicable to that device only. An alias defined on a profile applies to every device using the profile. Similarly, aliases defined at the RF Domain level apply to all devices within that domain.

Aliases defined at any given level can be overridden at any of the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.

Aliases can be classified as:

- address-range alias – Maps a name to a range of IP addresses. An address-range alias can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location’s network range is 172.16.13.20 through 172.16.13.110, the remote location’s ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

- host alias – Maps a name to a specific host (identified by its IP address. For example, 192.168.10.23). A host alias can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location’s local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

- network alias – Maps a name to a network. A network alias can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location’s network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

- network-group alias – Maps a name to a single or a range of addresses of devices, hosts, and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20.

  A network-group alias can contain a maximum of eight (8) host entries, eight (8) network entries, and eight (8) IP address-range entries. A maximum of 32 network-group alias entries can be created.

  A network-group alias can be used in IP firewall rules to substitute hosts, subnets, and IP address ranges.

- network-service alias – Maps a name to service protocols and ports to match. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network-service alias. When used with an ACL, the network-service alias defines the service-specific components of the ACL rule. Overrides can be applied to the service alias, at the device level, without modifying the ACL. Application of overrides to the service alias allows an ACL to be used across sites.
Use a network-service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

NOTE: When used with ACLs, network, network-group, and network-service aliases act as enhanced firewalls.

- **number alias** – Maps a name to a number
- **vlan alias** – Maps a name to a VLAN ID. A VLAN alias can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.
- **string alias** – Maps a name to a specific string (for example, RF Domain name). A host alias can be utilized at different deployments. For example, if the main domain at a remote location is called `loc1.domain.com` and at another deployment location it is called `loc2.domain.com`, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the `loc1.domain.com` domain and at the other with the `loc2.domain.com` domain.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
alias [address-range|host|network|network-group|network-service|number|string|vlan]
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
alias host <HOST-ALIAS-NAME> <HOST-IP>
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP>] [host <HOST-IP>] [network <NETWORK-ADDRESS/MASK>]
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|ntp|nntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}
alias number <NUMBER-ALIAS-NAME> <0-4294967295>
alias string <STRING-ALIAS-NAME> <LINE>
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

**Parameters**

- alias address-range `<ADDRESS-RANGE-ALIAS-NAME>` `<STARTING-IP>` to `<ENDING-IP>`

| address-range `<ADDRESS-RANGE-ALIAS-NAME>` | Creates a address range alias, defining a range of IP addresses
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>&lt;ADDRESS-RANGE-ALIAS-NAME&gt;</code> – Specify the address range alias name.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Alias name should begin with `$`.  

---

NOTE: When used with ACLs, network, network-group, and network-service aliases act as enhanced firewalls.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| alias host `<HOST-ALIAS-NAME>` `<HOST-IP>` | Associates the network host's IP address with this host alias. For example, 'alias host $HOST 1.1.1.100'. In this example, the host alias name is: $HOST and the host IP address it is mapped to is: 1.1.1.100.  
  - `<HOST-IP>` – Specify the network host's IP address. |
| alias network `<NETWORK-ALIAS-NAME>` `<NETWORK-ADDRESS/MASK>` | Associates a single network with this network alias. For example, 'alias network $NET 1.1.1.0/24'. In this example, the network alias name is: $NET and the network it is mapped to is: 1.1.1.0/24.  
  - `<NETWORK-ADDRESS/MASK>` – Specify the network's address and mask. |
| alias network-group `<NETWORK-GROUP-ALIAS-NAME>` [address-range `<STARTING-IP>` to `<ENDING-IP>` | Associates a range of IP addresses with this network-group alias  
  - `<STARTING-IP>` – Specify the first IP address in the range.  
  - to `<ENDING-IP>` – Specify the last IP address in the range.  
  - `<STARTING-IP>` to `<ENDING-IP>` – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured. |
| network `<NETWORK-GROUP-ALIAS-NAME>` | Associates a single or multiple networks with this network-group alias  
  - `<NETWORK-ADDRESS/MASK>` – Specify the network's address and mask.  
  - `<NETWORK-ADDRESS/MASK>` – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured. |
### GLOBAL CONFIGURATION COMMANDS 4-13

**alias network-service** `<NETWORK-SERVICE-ALIAS-NAME>` *proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|ntp|ntp|pop3|proto|sip|smtp|sourceport (<1-65535>|<WORD>|ssh|telnet|tftp|www)>}

<table>
<thead>
<tr>
<th>alias network-service <code>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</code></th>
<th>Configures an alias that specifies available network services and the corresponding source and destination software ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</code> – Specify a network-service alias name.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Alias name should begin with <code>$</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level.</td>
<td></td>
</tr>
</tbody>
</table>

**proto [0-254]|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp]**

| proto [0-254]| <WORD>|eigrp|gre|igmp|igp|ospf|vrrp) | Use one of the following options to associate an Internet protocol with this network-service alias: |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| • `0-254` – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the Protocol field of the IPv4 header and the Next Header field of IPv6 header. For example, the User Datagram Protocol's (UDP) designated number is 17. |
| • `<WORD>` – Identifies the protocol by its name. Specify the protocol name. |
| • `gre` – Selects Generic Routing Encapsulation (GRE). The protocol number is 47. |
| • `igmp` – Selects Internet Group Management Protocol (IGMP). The protocol number is 2. |
| • `igp` – Selects Interior Gateway Protocol (IGP). The protocol number is 9. |
| • `ospf` – Selects Open Shortest Path First (OSPF). The protocol number is 89. |
| • `vrrp` – Selects Virtual Router Redundancy Protocol (VRRP). The protocol number is 112. |

{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|ntp|ntp|pop3|proto|sip|smtp|sourceport (<1-65535>|<WORD>|ssh|telnet|tftp|www)}

| `<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|ntp|ntp|pop3|proto|sip|smtp|sourceport (<1-65535>|<WORD>|ssh|telnet|tftp|www)> | After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports. |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| • `1-65535` – Optional. Configures a destination port number from 1 - 65535 |
| • `<WORD>` – Optional. Identifies the destination port by the service name provided. For example, the secure shell (SSH) service uses TCP port 22. |
| • `bgp` – Optional. Configures the default Border Gateway Protocol (BGP) services port (179) |
| • `dns` – Optional. Configures the default Domain Name System (DNS) services port (53) |

Contd..
• **ftp** – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21)
• **ftp-data** – Optional. Configures the default FTP data services port (20)
• **gopher** – Optional. Configures the default gopher services port (70)
• **https** – Optional. Configures the default HTTPS services port (443)
• **ldap** – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389)
• **nntp** – Optional. Configures the default *Newsgroup* (NNTP) services port (119)
• **ntp** – Optional. Configures the default *Network Time Protocol* (NTP) services port (123)
• **POP3** – Optional. Configures the default *Post Office Protocol* (POP3) services port (110)
• **proto** – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.
• **sip** – Optional. Configures the default *Session Initiation Protocol* (SIP) services port (5060)
• **smtp** – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) services port (25)
• **sourceport [<1-65535>|<WORD>]** – Optional. After specifying the destination port, you may specify a single or range of source ports.
  • **<1-65535>** – Specify the source port from 1 - 65535.
  • **<WORD>** – Specify the source port range, for example 1-10.
• **ssh** – Optional. Configures the default SSH services port (22)
• **telnet** – Optional. Configures the default Telnet services port (23)
• **tftp** – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)
• **www** – Optional. Configures the default HTTP services port (80)

---

**alias number <NUMBER-ALIAS-NAME> <0-4294967295>**

| alias number <NUMBER-ALIAS-NAME> <0-4294967295> | Creates a number alias identified by the <NUMBER-ALIAS-NAME> keyword. Number aliases map a name to a numeric value. For example, ‘alias number $NUMBER 100’
| | • The number alias name is: $NUMBER
| | • The value assigned is: 100
| | The value referenced by alias $NUMBER, wherever used, is 100.
| | • <NUMBER-ALIAS-NAME> – Specify the number alias name.
| | • <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.

**Note:** Alias name should begin with ‘$’.  

---
### Global Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| alias string <STRING-ALIAS-NAME> <LINE> | Creates a string alias identified by the `<STRING-ALIAS-NAME>` keyword.  
* `<STRING-ALIAS-NAME>` – Specify the string alias name.  
* `<LINE>` – Specify the string value.  
**Note:** String aliases map a name to an arbitrary string value. For example, 'alias string $DOMAIN test.example_company.com'.  
  - The string alias name is: `$DOMAIN`  
  - The value assigned is: test.example_company.com (a domain name)  
  - The value referenced by alias `$DOMAIN`, wherever used, is test.example_company.com.  
* **Note:** Alias name should begin with `$`. |
| alias vlan <VLAN-ALIAS-NAME> <1-4094> | Creates a VLAN alias identified by the `<VLAN-ALIAS-NAME>` keyword.  
* `<VLAN-ALIAS-NAME>` – Specify the VLAN alias name.  
**Note:** Alias name should begin with `$`.  
* `<1-4094>` – Specify the VLAN ID from 1 - 4094. |

### Examples

```bash
rfs4000-229D58(config)#alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
rfs4000-229D58(config)#alias network $TestNetworkAlias 192.168.13.0/24
rfs4000-229D58(config)#alias host $TestHostAlias 192.168.13.10
rfs4000-229D58(config)#alias vlan $TestVLANAlias 1
rfs4000-229D58(config)#alias network-group $TestNetGrpAlias address-range 192.168.13.7 to 192.168.13.16 192.168.13.20 to 192.168.13.25
rfs4000-229D58(config)#commit
rfs4000-229D58(config)#alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
rfs4000-229D58(config)#commit
rfs4000-229D58(config)#alias network-service $NetworkServAlias proto 17
rfs4000-229D58(config)#commit
rfs4000-229D58(config)#show context
```

<table>
<thead>
<tr>
<th>Line 1</th>
<th>Line 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
</tbody>
</table>

---

### Note

**String aliases** map a name to an arbitrary string value. For example, 'alias string $DOMAIN test.example_company.com'.

- **String alias name**: `$DOMAIN`  
- **Value assigned**: test.example_company.com (a domain name)  
- **Value referenced by alias**: test.example_company.com

**Note:** Alias name should begin with `$`.
**Example 1:**
rfs4000-229D58(config)#alias network-group $test host 192.168.1.10 192.168.1.11
rfs4000-229D58(config)#alias network-group $test network 192.168.2.0/24 192.168.3.0/24
rfs4000-229D58(config)#alias network-group $test address-range 192.168.4.10 to 192.168.4.20

In the preceding example, the network-group alias '$test' includes hosts 192.168.1.10 and 192.168.1.11, networks 192.168.2.0/24 and 192.168.3.0/24 and address-range 192.168.4.10 to 192.168.4.20.

**Example 2:**
rfs4000-229D58(config)#alias network-service $kerberos proto tcp 749 750 80 proto tcp sourceport 20 proto udp 68 sourceport 67

rfs4000-229D58(config)#commit

In the preceding example, the network-service alias '$kerberos' is configured to allow following traffic:

- TCP traffic to destination ports 749, 750, and 80
- TCP traffic from source port 20
- UDP traffic to destination port 68 and from source port 67
4.1.3 aaa-tacacs-policy

Global Configuration Commands

Configures AAA Terminal Access Controller Access-Control System (TACACS) policy. This policy configures multiple servers for authentication and authorization. A TACACS Authentication server should be configured when the server preference is authenticated server.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>

Parameters
- aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>

Examples
rfs7000-37FABE(config)#aaa-tacacs-policy testpolicy
rfs7000-37FABE(config-aaa-tacacs-policy-testpolicy)#?

AAA TACACS Policy Mode commands:
- accounting Configure accounting parameters
- authentication Configure authentication parameters
- authorization Configure authorization parameters
- no Negate a command or set its defaults
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-aaa-tacacs-policy-testpolicy)#

Related Commands

| no | Removes an existing AAA TACACS policy |

NOTE: For more information on the AAA-TACACS policy commands, see Chapter 25, AAA-TACACS-POLICY.
4.1.4 ap621

*Global Configuration Commands*

Adds an AP621 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ap621 <MAC>`

**Parameters**

- `ap621 <MAC>`

**Examples**

```plaintext
rfs7000-37FABE(config)#ap621 5C-0E-8B-E3-C3-56
rfs7000-37FABE(config-device-5C-0E-8B-E3-C3-56)#show context
ap621 5C-0E-8B-E3-C3-56
use profile default-ap621
use rf-domain default
hostname ap621-E3C356
rfs7000-37FABE(config-device-5C-0E-8B-E3-C3-56)#

rfs7000-37FABE(config)#show wireless ap configured
---------------------------------------------------------------------------------------
IDX   NAME                MAC              PROFILE       RF-DOMAIN    ADOPTED-BY
---------------------------------------------------------------------------------------
1     ap621-E3C356        5C-0E-8B-E3-C3-56 default-ap621 default un-adopted
---------------------------------------------------------------------------------------
```

**Related Commands**

- `no` Removes an AP621 from the network
### 4.1.5 ap622

*Global Configuration Commands*

Adds an AP622 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ap622 <MAC>`

**Parameters**

- `ap622 <MAC>`

  - `<MAC>` Specify the AP622’s MAC address.

**Examples**

```bash
rfs7000-37FABE(config)#ap622 B4-C7-99-43-C3-DC
rfs7000-37FABE(config-device-B4-C7-99-43-C3-DC)#show context
ap622 B4-C7-99-43-C3-DC
  use profile default-ap622
  use rf-domain default
  hostname ap622-43C3DC
rfs7000-37FABE(config-device-B4-C7-99-43-C3-DC)#
rfs7000-37FABE(config)#show wireless ap configured
```

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap621-E3C356</td>
<td>5C-0E-8B-E3-C3-56</td>
<td>default-ap621</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap622-43C3DC</td>
<td>B4-C7-99-43-C3-DC</td>
<td>default-ap622</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

**Related Commands**

`no` Removes an AP622 from the network
4.1.6 ap650

Global Configuration Commands

Adds an AP650 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
ap650 <MAC>

Parameters
- ap650 <MAC>

Examples
rfs7000-37FABE(config)#ap650 5C-0E-8B-34-81-BC
rfs7000-37FABE(config-device-5C-0E-8B-34-81-BC)#show context
ap650 5C-0E-8B-34-81-BC
    use profile default-ap650
    use rf-domain default
    hostname ap650-3481BC
rfs7000-37FABE(config-device-5C-0E-8B-34-81-BC)#
rfs7000-37FABE(config)#show wireless ap configured

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap621-E3C356</td>
<td>5C-0E-8B-E3-C3-56</td>
<td>default-ap621</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap622-43C3DC</td>
<td>B4-C7-99-43-C3-DC</td>
<td>default-ap622</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</td>
<td>ap650-3481BC</td>
<td>5C-0E-8B-34-81-BC</td>
<td>default-ap650</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#

Related Commands

no

Remove an AP650 from the network
4.1.7 ap6511

Global Configuration Commands

Adds an AP6511 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ap6511 <MAC>

Parameters

- <MAC> Specify the AP6511’s MAC address.

Examples

rfs7000-37FABE(config)#ap6511 5C-0E-8B-08-45-6A
rfs7000-37FABE(config-device-5C-0E-8B-08-45-6A)#show context
ap6511 5C-0E-8B-08-45-6A
use profile default-ap6511
use rf-domain default
hostname ap6511-08456A
license AAP DEFAULT-LICENSE
rfs7000-37FABE(config-device-5C-0E-8B-08-45-6A)#

rfs7000-37FABE(config)#show wireless ap configured

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap621-E3C356</td>
<td>5C-0E-8B-E3-C3-56</td>
<td>default-ap621</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap622-43C3DC</td>
<td>B4-C7-99-43-C3-DC</td>
<td>default-ap622</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</td>
<td>ap650-3481BC</td>
<td>5C-0E-8B-34-81-BC</td>
<td>default-ap650</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>4</td>
<td>ap6511-08456A</td>
<td>5C-0E-8B-08-45-6A</td>
<td>default-ap6511</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#

Related Commands

no Removes an AP6511 from the network
### 4.1.8 ap6521

**Global Configuration Commands**

Adds an AP6521 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
ap6521 <MAC>
```

**Parameters**

- `ap6521 <MAC>`

**Examples**

```plaintext
nx9500-6C8809(config)#ap6521 FC-0A-81-42-93-6C
nx9500-6C8809(config-device-FC-0A-81-42-93-6C)#show context
```

**Related Commands**

- `no` Removes an AP6521 from the network
4.1.9 ap6522

**Global Configuration Commands**

Adds an AP6522 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap6522 <MAC>
```

**Parameters**

- `ap6522 <MAC>`

| <MAC> | Specify the AP6522’s MAC address.

**Examples**

```
nx9500-6C8809(config)#ap6522 B4-C7-99-58-72-58
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#show context
ap6522 B4-C7-99-58-72-58
use profile default-ap6522
use rf-domain default
hostname ap6522-587258
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#
```

```
nx9500-6C8809(config)#show wireless ap configured
```

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap6521-42936C</td>
<td>FC-0A-81-42-93-6C</td>
<td>default-ap6521</td>
<td>default</td>
<td>B4-C7-99-6C-88-09</td>
</tr>
<tr>
<td>2</td>
<td>ap6522-587258</td>
<td>B4-C7-99-58-72-58</td>
<td>default-ap6522</td>
<td>default</td>
<td>B4-C7-99-6C-88-09</td>
</tr>
</tbody>
</table>

```
nx9500-6C8809(config)#
```

**Related Commands**

- `no` Removes an AP6522 from the network
4.10 ap6532

Global Configuration Commands

Adds an AP6532 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ap6532 <MAC>

Parameters

- <MAC>

Examples

```
nx9500-6C8809(config)#ap6532 00-23-68-31-16-59
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#show context
ap6532 00-23-68-31-16-59
use profile default-ap6532
use rf-domain default
hostname ap6532-311659
nx9500-6C8809(config-device-00-23-68-31-16-59)#
nx9500-6C8809(config)#show wireless ap configured
```

```
IDX   NAME                MAC             PROFILE      RF-DOMAIN       ADOPTED-BY
---------------------------------------------------------------------------------------
1   ap6521-42936C      FC-0A-81-42-93-6C   default-ap6521     default     B4-C7-99-6C-88-09
2  ap6522-587258     B4-C7-99-58-72-58   default-ap6522    default   B4-C7-99-6C-88-09
3  ap6532-311659      00-23-68-31-16-59   default-ap6532    default   B4-C7-99-6C-88-09
---------------------------------------------------------------------------------------
nx9500-6C8809(config)#
```

Related Commands

- **<MAC>** Specify the AP6532’s MAC address.
- **no** Removes an AP6532 from the network
4.1.11 ap6562

Global Configuration Commands

Adds an AP6562 to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
ap6562 <MAC>

Parameters
- ap6562 <MAC>

Examples
nx9500-6C8809(config)#ap6562 00-23-09-0E-12-60
nx9500-6C8809(config-device-00-23-09-0E-12-60)#show context
ap6562 00-23-09-0E-12-60
use profile default-ap6562
use rf-domain default
hostname ap6562-0E1260

nx9500-6C8809(config)#show wireless ap configured

IDX  NAME             MAC             PROFILE      RF-DOMAIN       ADOPTED-BY
1    ap6521-42936C    FC-0A-81-42-93-6C default-ap6521  default  B4-C7-99-6C-88-09
2    ap6522-587258    B4-C7-99-58-72-58  default-ap6522  default  B4-C7-99-6C-88-09
3    ap6532-311659    00-23-68-31-16-59  default-ap6532  default  B4-C7-99-6C-88-09
4    ap6562-0E1260    00-23-09-0E-12-60  default-ap6562  default  B4-C7-99-6C-88-09

nx9500-6C8809(config)#

Related Commands

no Removes an AP6562 from the network
4.1.12 ap71xx

- **Global Configuration Commands**

  Adds an AP71XX series to the network. If a profile for the AP is not available, a new profile is created.

  Supported in the following platforms:
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap71xx <MAC>
```

**Parameters**

- `ap71xx <MAC>`

**Examples**

```
nx4500-5CFA2B(config)#ap71xx 00-23-68-11-E6-C4
nx4500-5CFA2B(config-device-00-23-68-11-E6-C4)#show context
ap71xx 00-23-68-11-E6-C4
  use profile default-ap71xx
  use rf-domain default
  hostname ap7131-11E6C4
nx4500-5CFA2B(config-device-00-23-68-11-E6-C4)#
```

```
nx4500-5CFA2B(config)#show wireless ap configured

IDX       NAME               MAC              PROFILE       RF-DOMAIN        ADOPTED-BY
---------------------------------------------------------------------------------------
1  ap7131-11E6C4 00-23-68-11-E6-C4  default-ap71xx  default  B4-C7-99-5C-FA-2B
2  rfs4000-229D58 00-23-68-22-9D-58  default-rfs4000  default
---------------------------------------------------------------------------------------
nx4500-5CFA2B(config)#
```

**Related Commands**

- `no` Removes an AP71XX from the network
### 4.1.13 ap7502

**Global Configuration Commands**

Adds an AP7502 series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
ap7502 <MAC>
```

**Parameters**

- `ap7502 <MAC>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>Specify the AP7502's MAC address.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#ap7502 00-23-68-99-BF-A8
rfs7000-37FABE(config-device-00-23-68-99-BF-A8)#
```

**Related Commands**

- `no`  | Removes an AP7502 from the network |
4.1.14 **ap7522**

*Global Configuration Commands*

Adds an AP7522 series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ap7522 <MAC>`

**Parameters**

- `ap7522 <MAC>`

<table>
<thead>
<tr>
<th>&lt;MAC&gt;</th>
<th>Specify the AP7522’s MAC address.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config)#ap7522 00-23-09-0E-12-63
rfs7000-37FABE(config-device-00-23-09-0E-12-63)#
```

**Related Commands**

- `no` Removes an AP7522 from the network
4.1.15 ap7532

Global Configuration Commands

Adds an AP7532 series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
ap7532 <MAC>

Parameters
- <MAC>

Examples
rfs7000-37FABE(config)#ap7532 00-23-09-0E-12-71
rfs7000-37FABE(config-device-00-23-09-0E-12-71)#

Related Commands
- no

Removes an AP7532 from the network
4.1.16 ap7562

Global Configuration Commands

Adds an AP7562 series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ap7562 <MAC>

Parameters

- ap7562 <MAC>

<table>
<thead>
<tr>
<th>&lt;MAC&gt;</th>
<th>Specify the AP7562’s MAC address.</th>
</tr>
</thead>
</table>

Examples

rfs7000-37FABE(config)#ap7562 84-24-8D-80-C2-AC
rfs7000-37FABE(config-device-84-24-8D-80-C2-AC)#

Related Commands

- **no** Removes an AP7562 from the network
4.1.17 ap81xx

*Global Configuration Commands*

Adds an AP81XX series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
ap81xx <MAC>

**Parameters**
- ap81xx <MAC>

<table>
<thead>
<tr>
<th>&lt;MAC&gt;</th>
<th>Specify the AP81XX's MAC address.</th>
</tr>
</thead>
</table>

**Examples**
rfs6000-81742D#ap81xx B4-C7-99-71-17-28
rfs6000-81742D(config-device-B4-C7-99-71-17-28)#show context
ap8132 B4-C7-99-71-17-28
use profile default-ap81xx
use rf-domain default
hostname ap8132-711728
license AAP DEFAULT-LICENSE
rfs6000-81742D(config-device-B4-C7-99-71-17-28)#
rfs6000-81742D(config)#show wireless ap configured

```
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap8132-711728</td>
<td>B4-C7-99-71-17-28</td>
<td>default-ap81xx</td>
<td>default</td>
<td>00-15-70-81-74-2D</td>
</tr>
</tbody>
</table>
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
```
rfs6000-81742D(config)#

**Related Commands**

*no* Removes an AP81XX from the network
4.1.18 ap82xx

Global Configuration Commands

Adds an AP82XX series to the network. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ap82xx <MAC>

Parameters

- ap82xx <MAC>

Parameters:

- <MAC> Specify the AP82XX’s MAC address.

Examples

rfs7000-37FABE(config-device-00-23-68-14-77-48)
rfs7000-37FABE(config-device-00-23-68-14-77-48)#show context
ap82xx 00-23-68-14-77-48
use profile default-ap82xx
use rf-domain default
hostname ap8232-147748
rfs7000-37FABE(config-device-00-23-68-14-77-48)#

rfs7000-37FABE(config)#show wireless ap configured

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap621-E3C356</td>
<td>5C-0E-8B-E3-C3-56</td>
<td>default-ap621</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap622-43C3DC</td>
<td>B4-C7-99-43-C3-DC</td>
<td>default-ap622</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</td>
<td>ap650-3481BC</td>
<td>5C-0E-8B-34-81-BC</td>
<td>default-ap650</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>4</td>
<td>ap6511-08456A</td>
<td>5C-0E-8B-08-45-6A</td>
<td>default-ap6511</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>5</td>
<td>ap8232-147748</td>
<td>00-23-68-14-77-48</td>
<td>default-ap82xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#

Related Commands

no

Removes an AP82XX from the network
### 4.1.19 application

The following table lists the commands that enable you to enter the Application definition configuration mode:

**Table 4.2 Application-Policy Config Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>Creates a new application definition and enters its configuration mode. This command allows you to create a customized application detection definition.</td>
<td>page 4-34</td>
</tr>
<tr>
<td>application-config-mode commands</td>
<td>Summarizes application definition configuration mode commands.</td>
<td>page 4-36</td>
</tr>
</tbody>
</table>
4.1.19.1 application

application

Creating a new application definition and enters its configuration mode. This command allows you to create a customized application recognition definition.

The WiNG software uses Protocol and Application Classification Engine (PACE), a third-party Deep Packet Inspection (DPI) engine from IPOQUE, to enable application recognition. When enabled, the PACE evaluation package inspects network traffic to determine the application/protocol type. It can detect common HTTP-based applications (for example, Youtube and Facebook), enterprise-based applications (for example, Lync and Webex), and peer-to-peer applications (for example Facetime and Bittorrent) in the network’s traffic. PACE uses a range of DPI technologies to identify approximately 700 built-in applications that are grouped into twenty two (22) application categories. You can use this command to add applications not included in the PACE package.

Application recognition can be used as a filter to classify packets based on their application/protocol type. Once classified, an action is applied, such as deny, allow, mark, or rate-limit on the packet. These actions are defined in an application policy. Therefore, an application policy, like an Access Control List (ACL), is a set of rules that control traffic within the managed network. The match criteria, used by the application policy, are the built-in PACE app-categories and/or the customized applications configured here.

NOTE: The PACE DPI engine has to be enabled to trigger application recognition. To enable DPI, in the device or profile configuration mode, execute the dpi command. To enable customized application detection, in the device/profile configuration mode execute the dpi > custom-app <APPLICATION-NAME> command. For more information, see dpi.

NOTE: To enable application recognition based traffic control, apply this application or PACE app-categories to an application policy, and use the policy with the RADIUS user authentication process, user role, WLAN, or bridge VLAN. For more information, see application-policy.

Supported in the following platforms:
- Access Points — AP7522, AP7532, AP7562
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

application <APPLICATION-NAME>

Parameters

- application <APPLICATION-NAME>

<table>
<thead>
<tr>
<th>application &lt;APPLICATION-NAME&gt;</th>
<th>Creates a new application definition and enters its configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;APPLICATION-NAME&gt; – Specify a name of the new application definition. It is created if not already existing in the system.</td>
<td></td>
</tr>
</tbody>
</table>
Examples

nx9500-6C8809(config)#application Bing
nx9500-6C8809(config-application-Bing)#?

Application Mode commands:

- **app-category**: Set application category (default is custom)
- **description**: Add application description
- **https**: Secure HTTP
- **no**: Negate a command or set its defaults
- **use**: Set setting to use

- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **do**: Run commands from Exec mode
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal

nx9500-6C8809(config-application-Bing)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Deletes an existing application definition</td>
</tr>
</tbody>
</table>
4.19.2 application-config-mode commands

The following table summarizes Application definition configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>app-category</td>
<td>Configures the category for this application definition</td>
<td>page 4-37</td>
</tr>
<tr>
<td>description</td>
<td>Configures a description for this application definition</td>
<td>page 4-38</td>
</tr>
<tr>
<td>https</td>
<td>Configures the HTTPS common-name attribute value for this application category’s server certificate. Applicable only to applications using HTTPS protocol.</td>
<td>page 4-39</td>
</tr>
<tr>
<td>use</td>
<td>Associates a network-service alias or a URL list with this application definition. Applicable for applications using protocols other than HTTPS.</td>
<td>page 4-40</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets this application definition’s configured settings</td>
<td>page 4-41</td>
</tr>
</tbody>
</table>
4.1.19.2.1  app-category

> application-config-mode commands

Configures the category for this application definition

Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
app-category <APP-CATEGORY-NAME>

Parameters

- app-category <APP-CATEGORY-NAME>

Examples
nx9500-6C8809(config-application-Bing)#app-category [TAB]

antivirus\ update    audio                business
conference            custom                database
filetransfer           gaming                generic
im                    mail                   mobile
network\ management   other                 p2p
remote\ control        social\ networking    standard
streaming             tunnel                video
voip                   web

nx9500-6C8809(config-application-Bing)#

nx9500-6C8809(config-application-Bing)#app-category streaming

nx9500-6C8809(config-application-Bing)#show context application Bing

app-category streaming

nx9500-6C8809(config-application-Bing)#

Related Commands

no  Resets application category to default (custom)
4.1.19.2.2  description

▸ application-config-mode commands

Configures a description for this application definition
Supported in the following platforms:
  • Access Points — AP7522, AP7532
  • Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
description <WORD>

Parameters
  • description <WORD>

<table>
<thead>
<tr>
<th>description &lt;WORD&gt;</th>
<th>Configures a description for this application</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify a description not exceeding 80 characters in length.</td>
</tr>
</tbody>
</table>

Examples
nx9500-6C8809(config-application-Bing)#description "Bing is Microsoft's Web search engine"

nx9500-6C8809(config-application-Bing)#show context application Bing
description "Bing is Microsoft's Web search engine"
app-category streaming
nx9500-6C8809(config-application-Bing)#

Related Commands

| no | Removes this description configured for this application |
4.1.19.2.3 https

application-config-mode commands

Configures the HTTPS common-name attribute value for this application category’s server certificate

Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

https server-cert common-name [contains|ends-with] <WORD>

Parameters

- https server-cert common-name [contains|ends-with] <WORD>

<table>
<thead>
<tr>
<th>https server-cert</th>
<th>Configures the HTTPS common-name attribute value for this application category’s server certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-name [contains</td>
<td>ends-with] &lt;WORD&gt;</td>
</tr>
<tr>
<td></td>
<td>• contains – Filters applications having common-name attributes containing the string specified here</td>
</tr>
<tr>
<td></td>
<td>• ends-with – Filters applications ending with the string specified here</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the string to match.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-application-Bing)#https server-cert common-name exact bing.com

nx9500-6C8809(config-application-Bing)#show context
application Bing
description "Bing is Microsoft's web search engine"
app-category streaming
https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#

Related Commands

no

Removes the HTTPS common-name attribute value configured with this application category
4.1.19.2.4 use

application-config-mode commands

Associates a network-service alias or a URL list with this application definition.

For applications using protocols other than HTTPS, use this command to define the protocols, ports, and/or URL host name to match.

Supported in the following platforms:
  - Access Points — AP7522, AP7532
  - Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]

Parameters
- use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]

<table>
<thead>
<tr>
<th>use</th>
<th>Configures this application definition to use a network-service alias or a URL list</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-service &lt;NETWORK-SERVICE-ALIAS-NAME&gt;</td>
<td>Associates a network-service alias with this application definition</td>
</tr>
<tr>
<td></td>
<td>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify the network-service alias name (should be existing and configured). The network-service alias should specify the protocols and ports to match.</td>
</tr>
<tr>
<td>url-list &lt;URL-LIST-NAME&gt;</td>
<td>Associates a URL list with this application definition</td>
</tr>
<tr>
<td></td>
<td>• &lt;URL-LIST-NAME&gt; – Specify the URL list name (should be existing and configured). The URL list should specify the HTTP URL host names to match.</td>
</tr>
</tbody>
</table>

Examples
nx9500-6C8809(config-application-Bing)#use url-list Bing
nx9500-6C8809(config-application-Bing)#show context application Bing
description "Bing is Microsoft's web search engine"
app-category streaming
use url-list Bing
https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#

Related Commands
- no
  - Removes the network-service alias or the URL list associated with this application definition
4.19.2.5  no

application-config-mode commands

Removes or resets this application definition’s configured settings

Supported in the following platforms:
  • Access Points — AP7522, AP7532
  • Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [app-category|description|https|use]

no [app-category|description]

no https server-cert common-name [contains|ends-with] <WORD>

no use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]

Parameters

• no <PARAMETERS>

no <PARAMETERS> Removes or resets this application definition’s configured settings based on the parameters passed

Examples

The following example displays the application definition ‘Bing’ parameters before the ‘no’ commands are executed:

```
nx9500-6C8809(config-application-Bing)#show context
application Bing
description "Bing is Microsoft's web search engine"
app-category streaming
use url-list Bing
https server-cert common-name exact bing.com
```
x9500-6C8809(config-application-Bing)#

```
nx9500-6C8809(config-application-Bing)#no description
```
x9500-6C8809(config-application-Bing)#

```
nx9500-6C8809(config-application-Bing)#no https server-cert common-name exact bing.com
```
x9500-6C8809(config-application-Bing)#

The following example displays the application definition ‘Bing’ parameters before the ‘no’ commands are executed:

```
nx9500-6C8809(config-application-Bing)#show context
application Bing
  app-category streaming
  use url-list Bing
```
x9500-6C8809(config-application-Bing)#
4.1.20 application-policy

The following table lists the commands that enable you to enter the Application policy configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>application-policy</td>
<td>Creates an application policy and enters its configuration mode</td>
<td>page 4-43</td>
</tr>
<tr>
<td>application-policy-mode commands</td>
<td>Summarizes the application policy configuration mode commands</td>
<td>page 4-45</td>
</tr>
</tbody>
</table>
4.1.20.1 application-policy

- **application-policy**

  Creates an application policy and enters its configuration mode

  An application policy defines actions to perform on a packet when it matches a specified set of pre-defined applications or application categories. These rules are numbered and are applied to each packet sequentially in increasing order of their precedence number. Once a match is made, the packet is either forwarded, dropped, marked, or rate limited depending on the action specified in that rule.

  Application recognition is the most important aspect of application-based traffic control and prioritization within a managed network. The WiNG software uses PACE, a third-party DPI engine from IPOQUE, to enable application recognition. When enabled, PACE uses various DPI technologies to identify a range of applications that include Web-based and other difficult-to-classify protocols utilizing dynamic TCP/UDP port assignments. When an application is recognized and classified, a pre-defined application policy invokes appropriate action for that specific application. PACE provides a default database of application definitions (approximately 700 canned application signatures). In addition, to these, there is a provision to add new customized application definitions. You can also customize the default, canned application definitions.

  To enable an application policy, apply it at one or all of the following levels within the network to enforce application assurance:

  - **RADIUS CoA usage** – In the device/profile configuration mode, use the `application-policy > radius > <APPLICATION-POLICY-NAME>` command to apply the policy to every user successfully authenticated by the RADIUS server.

  - **User role** – In the role-policy-user-role configuration mode, use the `use > application-policy <APPLICATION-POLICY-NAME>` command to apply the policy to all users assigned to the role.

  - **WLAN** – In the WLAN configuration mode, use the `use > application-policy <APPLICATION-POLICY-NAME>` command to apply the policy to all users accessing the WLAN.

  - **Bridge VLAN** – In the bridge VLAN configuration mode, use the `use > application-policy <APPLICATION-POLICY-NAME>` command to apply the policy for the traffic corresponding to the bridged VLAN.

  Supported in the following platforms:

  - Access Points — AP7522, AP7532
  - Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
application-policy <APPLICATION-POLICY-NAME>
```

**Parameters**

- **application-policy <APPLICATION-POLICY-NAME>**

| application-policy <APPLICATION-POLICY-NAME> | Specify the application policy name. If the policy does not exist, it is created. |
Examples

nx9500-6C8809(config)#application-policy TestApplicPolicy
nx9500-6C8809(config-app-policy-TestApplicPolicy)#?

Application Policy Mode commands:

allow Allow packets
deny Deny packets
description Application policy description
enforcement-time Configure policy enforcement based on time
logging Application recognition logging
mark Mark packets
no Negate a command or set its defaults
rate-limit Rate-limit packets

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

nx9500-6C8809(config-app-policy-TestApplicPolicy)#

Related Commands

| no | Removes an existing application policy |
4.1.20.2 application-policy-mode commands

The following table summarizes Application policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>Creates an allow rule and configures the match criteria based on which</td>
<td>page 4-46</td>
</tr>
<tr>
<td></td>
<td>packets are filtered and the allow access action applied</td>
<td></td>
</tr>
<tr>
<td>deny</td>
<td>Creates a deny rule and configures the match criteria based on which</td>
<td>page 4-48</td>
</tr>
<tr>
<td></td>
<td>packets are filtered and the deny access action applied</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>Configures a brief description for this application policy that enables you</td>
<td>page 4-50</td>
</tr>
<tr>
<td></td>
<td>to differentiate it from other application policies</td>
<td></td>
</tr>
<tr>
<td>enforcement-</td>
<td>Configures an enforcement time period in days and hours for this application</td>
<td>page 4-51</td>
</tr>
<tr>
<td>time</td>
<td>policy. The policy is enforced only during the specified time period.</td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td>Enables logging of application recognition hits made by the PACE DPI engine.</td>
<td>page 4-52</td>
</tr>
<tr>
<td></td>
<td>It also sets the logging level.</td>
<td></td>
</tr>
<tr>
<td>mark</td>
<td>Creates a mark rule and configures the match criteria based on which</td>
<td>page 4-53</td>
</tr>
<tr>
<td></td>
<td>packets are filtered and marked with 802.1p priority value or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Differentiated Service Code Point (DSCP) code</td>
<td></td>
</tr>
<tr>
<td>rate-limit</td>
<td>Creates a rate-limit rule and configures the match criteria based on which</td>
<td>page 4-55</td>
</tr>
<tr>
<td></td>
<td>incoming and outgoing packets are filtered and the configured rate limits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>applied</td>
<td></td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets this application policy’s settings</td>
<td>page 4-57</td>
</tr>
</tbody>
</table>
### 4.1.20.2.1 allow

> application-policy-mode commands

Creates an allow rule and configures the match criteria based on which packets are filtered and the allow access action applied.

Supported in the following platforms:
- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
precedence <1-256>
```

**Parameters**

- **allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]**
  - `app-category` Uses application category as the match criteria
    - `<APP-CATEGORY-NAME>` – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote\ control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system forwards the packet or else drops it.
    - `all` – The system forwards all packets irrespective of the application category.
  - `application` Uses application name as the match criteria
    - `<APPLICATION-NAME>` – Specify the application name. Each packet’s application is matched with the application name specified here. In case of a match, the system forwards the packet.

**Note:** The WiNG database provides approximately 381 canned applications. In addition to these, the database also includes custom-made applications. These are application definitions created using the `application` command.

- **precedence <1-256>**
  - Assigns a precedence value for this allow rule. The precedence value differentiates between rules applicable to applications and the application categories to which they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.

Let us consider application `youtube` belonging to app-category `streaming`. The action required is: Allow `youtube` packets and deny all other applications belonging to app-category `streaming`.

The rules can be defined as:

```
#allow application youtube precedence 1
#deny app-category streaming precedence 2
```

Contd..
The following configuration is incorrect:
```plaintext
#deny app-category streaming precedence 1
#allow application youtube precedence 2
```
Once the `deny` app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent `allow` rule.

Note: The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
</table>
| The following examples show two `allow` rules, allowing access to all packets belonging to the application category ‘business’ and the application ‘Bing’:
```
x9500-6C8809(config-app-policy-Bing)#allow application Bing [TAB]
Bing
BitTorrent                BitTorrent_encrypted
BitTorrent_plain          BitTorrent_uTP            BitTorrent_uTP_encrypted
nx9500-6C8809(config-app-policy-Bing)#
```

Note: Bing is not one of the WiNG built-in database applications. It is a customized application created using the `application` command.
```
x9500-6C8809(config-app-policy-Bing)#allow application Bing precedence 1
nx9500-6C8809(config-app-policy-Bing)#allow app-category business [TAB]
all    antivirus\ update    audio
business    conference    custom
database    filetransfer    gaming
generic    im    mail
mobile     network\ management    other
p2p     remote_control    social\ networking
standard    streaming    tunnel
video    voip    web
nx9500-6C8809(config-app-policy-Bing)#
```
```
x9500-6C8809(config-app-policy-Bing)#allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#show context application-policy Bing
allow application Bing precedence 1
allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#
```

Related Commands
```
no
Removes this allow rule from the application policy
```
### 4.1.20.2.2 deny

**application-policy-mode commands**

Creates a deny rule and configures the match criteria based on which packets are filtered and the deny access action applied.

**Syntax**

```
deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
    precedence <1-256>
```

**Parameters**

- `deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
  precedence <1-256>`

<table>
<thead>
<tr>
<th>deny</th>
<th>Creates a deny rule and configures the match criteria. The options are app-category and application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>app-category [&lt;APP-CATEGORY-NAME&gt;</td>
<td>all]</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;APP-CATEGORY-NAME&gt;</code> – Specify the application category name. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote\ control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet’s app-category is matched with the value specified here. In case of a match, the system drops the packet.</td>
</tr>
<tr>
<td></td>
<td>• <code>all</code> – The system drops all packets irrespective of the application category.</td>
</tr>
<tr>
<td>application &lt;APPLICATION-NAME&gt;</td>
<td>Uses application name as the match criteria.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;APPLICATION-NAME&gt;</code> – Specify the application name. Each packet’s application is matched with the application name specified here. In case of a match, the system drops the packet.</td>
</tr>
<tr>
<td>precedence &lt;1-256&gt;</td>
<td>Assigns a precedence value for this deny rule. The precedence value differentiates between rules applicable to applications and the application categories to which they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule. Let us consider application <code>youtube</code> belonging to app-category <code>streaming</code>. The action required is: Allow <code>youtube</code> packets and deny all other applications belonging to app-category <code>streaming</code>. The rules can be defined as:</td>
</tr>
<tr>
<td></td>
<td>#allow application youtube precedence 1</td>
</tr>
<tr>
<td></td>
<td>#deny app-category streaming precedence 2</td>
</tr>
<tr>
<td></td>
<td>The following configuration is incorrect:</td>
</tr>
<tr>
<td></td>
<td>#deny app-category streaming precedence 1</td>
</tr>
<tr>
<td></td>
<td>#allow application youtube precedence 2</td>
</tr>
<tr>
<td></td>
<td>Once the <code>deny</code> app-category streaming precedence 1 rule is hit, all streaming packets, including <code>youtube</code>, are dropped. Consequently, there are no packets left to apply the subsequent <code>allow</code> rule.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.</td>
</tr>
</tbody>
</table>
Examples
The following example shows one deny rule, denying access to all packets belonging to the application category 'social networking':

```plaintext
nx9500-6C8809(config-app-policy-Bing)#deny app-category social networking precedence 3
```

```plaintext
nx9500-6C8809(config-app-policy-Bing)#show context application-policy Bing
  allow application Bing precedence 1
  allow app-category business precedence 2
  deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

Note, In the preceding example, none of the allow and deny rules apply to the same application or app-category.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes this deny rule from the application policy</td>
</tr>
</tbody>
</table>
4.1.20.2.3 description

application-policy-mode commands

Configures a brief description for this application policy that enables you to differentiate it from other application policies.

Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

description <LINE>

Parameters

- description <LINE>

<table>
<thead>
<tr>
<th>description &lt;LINE&gt;</th>
<th>Configures this application policy’s description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;LINE&gt;</td>
<td>– Specify a brief description not exceeding 80 characters in length.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-app-policy-Bing)#description "This application policy allows Bing search engine packets"

nx9500-6C8809(config-app-policy-Bing)#show context

application-policy Bing
description "This application policy allows Bing search engine packets"
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3

nx9500-6C8809(config-app-policy-Bing)#

Related Commands

| no | Removes this application policy’s description |
4.1.20.2.4 enforcement-time

`application-policy-mode commands`

Configures an enforcement time period in days and hours for this application policy. The policy is enforced only during the specified time period.

Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start-time <HH:MM> end-time <HH:MM>}
```

**Parameters**

- `enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start-time <HH:MM> end-time <HH:MM>}`

<table>
<thead>
<tr>
<th>enforcement-time days</th>
<th>Enforces this application policy on only the days specified here</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sunday – Enforces the policy only on Sundays</td>
</tr>
<tr>
<td></td>
<td>monday – Enforces the policy only on Mondays</td>
</tr>
<tr>
<td></td>
<td>tuesday – Enforces the policy only on Tuesdays</td>
</tr>
<tr>
<td></td>
<td>wednesday – Enforces the policy only on Wednesdays</td>
</tr>
<tr>
<td></td>
<td>thursday – Enforces the policy only on Thursdays</td>
</tr>
<tr>
<td></td>
<td>friday – Enforces the policy only on Fridays</td>
</tr>
<tr>
<td></td>
<td>saturday – Enforces the policy only on Saturdays</td>
</tr>
<tr>
<td></td>
<td>all – Enforces the policy only on all days</td>
</tr>
<tr>
<td></td>
<td>weekends – Enforces the policy only on weekends</td>
</tr>
<tr>
<td></td>
<td>weekdays – Enforces the policy only on weekdays</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>start-time <a href="">HH:MM</a></th>
<th>Optional. Configures this application policy’s enforcement period</th>
</tr>
</thead>
<tbody>
<tr>
<td>end-time <a href="">HH:MM</a></td>
<td>• start-time – Configures the start time. This is the time at which the application policy enforcement begins.</td>
</tr>
<tr>
<td></td>
<td>• end-time – Configures the end time. This is the time at which the application policy enforcement ends.</td>
</tr>
<tr>
<td></td>
<td>• <a href="">HH:MM</a> – Specify the start and end time in the HH:MM format.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-app-policy-Bing)#enforcement-time days weekdays start-time 10:30 end-time 20:00

nx9500-6C8809(config-app-policy-Bing)#show context application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 10:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
```

**Related Commands**

- `no` Removes this application policy’s enforcement period
4.1.20.2.5 logging

Enable logging of application recognition hits made by the PACE DPI engine. It also sets the logging level. Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

logging [level|on]

logging on

logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]

**Parameters**

- logging on
  - Enables logging of application recognition hits made by the PACE DPI engine. This option is disabled by default.

- logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]
  - Sets the logging level for application recognition hits made by the PACE DPI engine. This option is disabled by default.
    - <0-7> — Sets the message logging severity level on a scale of 0 - 7
    - emergencies – Severity level 0: System is unusable
    - alerts – Severity level 1: Requires immediate action
    - critical – Severity level 2: Critical conditions
    - errors – Severity level 3: Error conditions
    - warnings – Severity level 4: Warning conditions
    - notifications – Severity level 5: Normal but significant conditions (this is the default setting)
    - informational – Severity level 6: Informational messages
    - debugging – Severity level 7: Debugging messages

**Examples**

nx9500-6C8809(config-app-policy-Bing)#logging level critical

nx9500-6C8809(config-app-policy-Bing)# show context application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
logging level critical

nx9500-6C8809(config-app-policy-Bing)#

**Related Commands**

- `no` - Resets the logging level to default (notifications). And the `no > logging > on` command disables DPI logging.
4.1.20.2.6 mark

application-policy-mode commands

Creates a mark rule and configures the match criteria based on which packets are marked.

Marks packets, matching a specified set of application categories or applications/protocols, with 802.1p priority level or Differentiated Services Code Point (DSCP) type of service (ToS) code. Marking packets is a means of identifying them for specific actions, and is used to provide different levels of service to different traffic types.

Supported in the following platforms:
• Access Points — AP7522, AP7532
• Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
[8021p <0-7>|dscp <0-63>] precedence <1-256>

Parameters
• mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
[8021p <0-7>|dscp <0-63>] precedence <1-256>

mark Creates a mark rule and configures the match criteria. When applied, the rule marks packets, matching the criteria configured here, with 802.1p priority value or DSCP code. The match criteria options are: app-category and application.

app-category [<APP-CATEGORY-NAME>|all] Uses application category as the match criteria
• <APP-CATEGORY-NAME> – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet’s app-category is matched with the value specified here. In case of a match, the system marks the packet.
• all – The system marks all packets irrespective of the application category.

application <APPLICATION-NAME> Uses application name as the match criteria
• <APPLICATION-NAME> – Specify the application name. Each packet’s application is matched with the application name specified here. In case of a match, the system marks the packet.

Note: The WiNG database provides approximately 381 canned applications. In addition to these, the database includes custom-made applications. These are application definitions created using the application command.

8021p <0-7> Marks packets matching the specified criteria with 802.1p priority value
• <0-7> – Specify a value from 0 - 7.

Note: The IEEE 802.1p signaling standard enables marking of layer 2 network traffic. Layer 2 network devices (such as switches), using 802.1p standards, group traffic into classes based on their 802.1p priority value, which is appended to the packet’s MAC header. In case of traffic congestion, packets with higher priority get precedence over lower priority packets and are forwarded first.

dscp <0-63> Marks packets matching the specified criteria with DSCP ToS code
• <0-63> – Specify a value from 0 - 63.

Note: The DSCP protocol marks layer 3 network traffic. Layer 3 network devices (such as routers) using DSCP, mark each layer 3 packet with a six-bit DSCP code, which is appended to the packet’s IP header. Each DSCP code is assigned a corresponding level of service, enabling packet prioritization.
precedence <1-256> Assigns a precedence value for this mark rule. The precedence value differentiates between rules applicable to applications and the application categories they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.

Let us consider application *youtube* belonging to app-category *streaming*.

The action required is: Allow *youtube* packets and deny all other applications belonging to app-category *streaming*.

The rules can be defined as:

```
#allow application youtube precedence 1
#deny app-category streaming precedence 2
```

The following configuration is incorrect:

```
#deny app-category streaming precedence 1
#allow application youtube precedence 2
```

Once the *deny* app-category streaming precedence 1 rule is hit, all streaming packets, including *youtube*, are dropped. Consequently, there are no packets left to apply the subsequent *allow* rule.

**Note:** The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

Examples

nx9500-6C8809(config-app-policy-Bing)#mark app-category video dscp 9 precedence 4

nx9500-6C8809(config-app-policy-Bing)#mark application facetime dscp 10 precedence 5

nx9500-6C8809(config-app-policy-Bing)#show context

application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
mark app-category video dscp 9 precedence 4
mark application facetime dscp 10 precedence 5
logging level critical

nx9500-6C8809(config-app-policy-Bing)#

Related Commands

```
no
```
Removes this mark rule from the application policy
4.1.20.2.7 rate-limit

application-policy-mode commands

Creates a rate-limit rule and configures the match criteria

Supported in the following platforms:
- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

rate-limit [app-category <APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] ([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> precedence <0-256>

Parameters

- rate-limit [app-category <APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] ([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> precedence <0-256>

rate-limit Creates a rate-limit rule and configures the match criteria. When applied, the rule applies a rate-limit to packets that match the criteria configured here. These packets could be incoming, outgoing, or both. The match criteria options are: app-category and application.

app-category <APP-CATEGORY-NAME>|all]

Uses application category as the match criteria

- <APP-CATEGORY-NAME> – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system rate-limits the packet.
- all – The system rate-limits all packets irrespective of the application category.

application <APPLICATION-NAME>

Uses application name as the match criteria

- <APPLICATION-NAME> – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system rate-limits the packet.

[egress|ingress] The egress and ingress parameters are recursive and can be used to rate limit either incoming, outgoing, or both incoming and outgoing traffic.

- egress – Selects the traffic type as outgoing
- ingress – Selects the traffic type as outgoing

Note: After selecting the traffic type (incoming/outgoing) configure the rate and maximum burst size.

rate <50-1000000>

The following parameters are common to the ‘egress’ and ‘ingress’ keywords:

- rate – Configures the rate limit, in Kbps, for both incoming and outgoing packets
- <50-1000000> – Specify the rate limit from 50 - 1000000 Kbps.

max-burst-size

The following parameters are common to the ‘egress’ and ‘ingress’ keywords:

- max-burst-size – Configures the maximum burst size, in Kbytes, for both incoming and outgoing packets
- <2-1024> – Specify the maximum burst size from 2 - 1024 Kbytes.
precedence <1-256>

Assigns a precedence value for this mark rule. The precedence value differentiates between rules applicable to applications and the application categories they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.

Let us consider application **youtube** belonging to app-category **streaming**.

The action required is: Allow **youtube** packets and deny all other applications belonging to app-category **streaming**.

The rules can be defined as:

```bash
#allow application youtube precedence 1
#deny app-category streaming precedence 2
```

The following configuration is incorrect:

```bash
#deny app-category streaming precedence 1
#allow application youtube precedence 2
```

Once the **deny** app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent **allow** rule.

**Note:** The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

---

**Examples**

nx9500-6C8809(config-app-policy-Bing)#rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
description "This application policy allows Bing search engine packets"

enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
mark app-category video dscp 9 precedence 4
mark application facetime dscp 10 precedence 5
rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6
logging level critical

nx9500-6C8809(config-app-policy-Bing)#

**Related Commands**

| **no** | Removes this rate-limit rule from the application policy |
4.1.20.2.8 no

application-policy-mode commands

Removes or resets this application policy’s settings

Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [allow|deny|description|enforcement-time|logging|mark|rate-limit]

no allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
   precedence <1-256>

no deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
   precedence <1-256>

no description

enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|
   weekends|weekdays]

no logging [level|on]

mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
   precedence <1-256>

rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
   precedence <0-256>

Parameters

- no <PARAMETERS>

   no <PARAMETERS> Removes or resets this application policy settings based on the parameters passed

Examples

The following example shows the application policy ‘Bing’ settings before the ‘no’ commands are executed:

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
   description "This application policy allows Bing search engine packets"
   enforcement-time days weekdays start-time 12:30 end-time 20:00
   allow application Bing precedence 1
   allow app-category business precedence 2
   deny app-category "social networking" precedence 3
   mark app-category video dscp 9 precedence 4
   mark application facetime dscp 10 precedence 5
   rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6
   logging level critical

nx9500-6C8809(config-app-policy-Bing)#

nx9500-6C8809(config-app-policy-Bing)#no allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#no deny app-category social networking precedence 3
The following example shows the application policy 'Bing' settings after the 'no' commands are executed:

```
 nx9500-6C8809(config-app-policy-Bing)#show context application-policy Bing
   description "This application policy allows Bing search engine packets"
   enforcement-time days weekdays start-time 12:30 end-time 20:00
   allow application Bing precedence 1
   mark app-category video dscp 9 precedence 4
   mark application facetime dscp 10 precedence 5
   rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6
   logging level critical
 nx9500-6C8809(config-app-policy-Bing)#
```
4.1.21 association-acl-policy

Global Configuration Commands

Configures an association ACL policy. This policy defines a list of devices allowed or denied access to the network.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>

Parameters
- association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>

Examples
rfs7000-37FABE(config)#association-acl-policy test
rfs7000-37FABE(config-assoc-acl-test)#?
Association ACL Mode commands:
  deny Specify MAC addresses to be denied
  no Negate a command or set its defaults
  permit Specify MAC addresses to be permitted
  clrscr Clears the display screen
  commit Commit all changes made in this session
  do Run commands from Exec mode
  end End current mode and change to EXEC mode
  exit End current mode and down to previous mode
  help Description of the interactive help system
  revert Revert changes
  service Service Commands
  show Show running system information
  write Write running configuration to memory or terminal

rfs7000-37FABE(config-assoc-acl-test)#

Related Commands
- no Resets values or disables commands

NOTE: For more information on the association-acl-policy, see Chapter 10, ASSOCIATION-ACL-POLICY.
4.1.22 auto-provisioning-policy

Global Configuration Commands

Configures an auto provisioning policy. This policy configures the automatic provisioning of device adoption. The policy configures how an AP is adopted based on its type.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>

Parameters

- auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>

Examples

rfs7000-37FABE(config)#auto-provisioning-policy test
rfs7000-37FABE(config-auto-provisioning-policy-test)#?

Auto-Provisioning Policy Mode commands:

- adopt Add rule for device adoption
- default-adoption Adopt devices even when no matching rules are found. Assign default profile and default rf-domain
- deny Add rule to deny device adoption
- evaluate-always Set the flag to evaluate the policy everytime, regardless of previous adoption status
- no Negate a command or set its defaults
- redirect Add rule to redirect device adoption
- upgrade Add rule for device upgrade
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-auto-provisioning-policy-test)#

Related Commands

- no Removes an existing Auto Provisioning policy

NOTE: For more information on the association-acl-policy, see Chapter 9, AUTO-PROVISIONING-POLICY.
4.1.23 bgp

Global Configuration Commands

Configures Border Gateway Protocol (BGP) settings

BGP is an inter-ISP routing protocol which establishes routing between Internet Service Providers (ISPs). ISPs use BGP to exchange routing and reachability information between Autonomous Systems (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An AS is a set of routers under the same administration that use Interior Gateway Protocol (IGP) and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a graceful close (all outstanding data is delivered before the connection is closed).

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list] <LIST-NAME>
```

Parameters
- bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list] <LIST-NAME>

| as-path-list <LIST-NAME> | Creates an AS path list and enters its configuration mode  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LIST-NAME&gt; – Provide the AS-PATH-LIST name.</td>
</tr>
</tbody>
</table>
| community-list <LIST-NAME> | Creates a community list and enters its configuration mode  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LIST-NAME&gt; – Provide the COMMUNITY-LIST name.</td>
</tr>
</tbody>
</table>
| extcommunity-list <LIST-NAME> | Creates an extended community list and enters its configuration mode  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LIST-NAME&gt; – Provide the EXTCOMMUNITY-LIST name.</td>
</tr>
</tbody>
</table>
| ip-access-list <LIST-NAME> | Creates a BGP IP access list and enters its configuration mode  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LIST-NAME&gt; – Provide the BGP IP-ACCESS-LIST name.</td>
</tr>
</tbody>
</table>
| ip-prefix-list <LIST-NAME> | Creates a BGP IP prefix list and enters its configuration mode  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LIST-NAME&gt; – Provide the BGP IP-PREFIX-LIST name.</td>
</tr>
</tbody>
</table>
Examples

```
nx4500-5CFA2B(config)#bgp ?
  as-path-list  BGP AS path list Configuration
  community-list Add a community list entry
  extcommunity-list Add a extended community list entry (EXPERIMENTAL)
  ip-access-list Add an access list entry
  ip-prefix-list Build a prefix list

nx4500-5CFA2B(config)#
```

```
nx4500-5CFA2B(config)#bgp as-path-list AS-TEST-PATH
nx4500-5CFA2B(config-bgp-as-path-list-AS-TEST-PATH)#?
```

BGP AS Path List Mode commands:
- `deny` Specify packets to reject
- `no` Negate a command or set its defaults
- `permit` Specify packets to forward
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
nx4500-5CFA2B(config-bgp-as-path-list-AS-TEST-PATH)#
```

Related Commands

| `no` | Modifies BGP settings, based on the parameters passed |

**NOTE:** For more information on configuring BGP Top-Level Objects (TLOs), see Chapter 28, BORDER GATEWAY PROTOCOL.
4.1.24 **bonjour-gw-discovery-policy**

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a local area network (LAN). Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

This command configures a Bonjour GW Discovery policy. The policy defines a list of services clients can discover across subnets. A maximum of 8 (eight) policies can be created on access points, wireless controllers, or service platforms.

When configured and applied, this feature enables discovery of Bonjour services on local and/or tunneled VLANs.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

**Parameters**

- `bonjour-gw-discovery-policy <POLICY-NAME>`

| <POLICY-NAME> | Specify the Bonjour GW Discovery policy name. If the policy does not exist, it is created. In the Bonjour GW Discovery policy configuration mode, use the allow-service keyword to configure the services that the Bonjour gateway is allowed to discover. A maximum of 16 (sixteen) service rules can be created. Optionally, you can restrict this facility for users on specific VLANs. To do so, specify the VLAN IDs. **Note:** Execute the `bonjour-gw-forwarding-policy` command to enable forwarding of Bonjour service responses across VLANs. **Note:** To associate a Bonjour GW Discovery policy with a WLAN, in the WLAN configure mode, execute the following command:

```
use > bonjour-gw-discovery-policy > <POLICY-NAME>
```

For more information see, `use`.

**Note:** To associate a Bonjour GW Discovery policy with a VLAN, in the interface VLAN configure mode, execute the following command:

```
use > bonjour-gw-discovery-policy > <POLICY-NAME>
```

For more information see, `use`.

**Note:** To associate a Bonjour GW Discovery policy with a user role, in the role-policy - user-role config mode, execute the following command:

```
use > bonjour-gw-discovery-policy > <POLICY-NAME>
```

For more information see, `use`.  

---
Examples
rfs7000-37FABE(config)#bonjour-gw-discovery-policy TestPolicy
rfs7000-37FABE(config-bonjour-gw-discovery-policy-TestPolicy)#?

commands:
allow-service  Allow Bonjour Service on local or tunneled vlan, Optionally
                VLAN IDs can be given so service will be discovered for those
                vlan only
no             Negate a command or set its defaults
clrscr         Clears the display screen
commit         Commit all changes made in this session
do             Run commands from Exec mode
derb End current mode and change to EXEC mode
help           Description of the interactive help system
revert         Revert changes
service        Service Commands
show           Show running system information
write          Write running configuration to memory or terminal

rfs7000-37FABE(config-bonjour-gw-discovery-policy-TestPolicy)#

Related Commands

| no          | Removes an existing Bonjour GW Discovery policy |
4.1.25 bonjour-gw-forwarding-policy

Configures a Bonjour GW Forwarding policy. When configured and applied on the controller, the policy defines the service VLANs (the VLANs on which Bonjour services are running) and client VLANs where clients are present. All Bonjour responses from service VLANs are forwarded to client VLANs. A maximum of 2 (two) policies can be created on a wireless controller or service platform. And only 1 (one) policy can be created on an access point.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
bonjour-gw-forwarding-policy <POLICY-NAME>
```

Parameters

- bonjour-gw-forwarding-policy <POLICY-NAME>

**Examples**

```
rfs7000-37FABE(config)#bonjour-gw-forwarding-policy TestPolicy
rfs7000-37FABE(config-bonjour-gw-forwarding-policy-TestPolicy)#?
commands:
  forward-bonjour-response   Forwards bonjour service response across vlans
  no                         Negate a command or set its defaults
  clrscr                     Clears the display screen
  commit                     Commit all changes made in this session
  do                         Run commands from Exec mode
  end                        End current mode and change to EXEC mode
  exit                       End current mode and down to previous mode
  help                       Description of the interactive help system
  revert                     Revert changes
  service                    Service Commands
  show                       Show running system information
  write                      Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-bonjour-gw-forwarding-policy-TestPolicy)#
```

**Related Commands**

| no | Removes an existing Bonjour GW Forwarding policy |
4.1.26 bonjour-gw-query-forwarding-policy

Global Configuration Commands

Configures a Bonjour GW Query Forwarding policy and enters its configuration mode. When created and applied, this policy enables forwarding of Bonjour queries across VLANs.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
bonjour-gw-query-forwarding-policy <POLICY-NAME>

Parameters
- bonjour-gw-query-forwarding-policy <POLICY-NAME>

Examples
rfs7000-37FABE(config)#bonjour-gw-query-forwarding-policy TestPolicy
rfs7000-37FABE(config-bonjour-gw-query-forwarding-policy-test)#?
(config-bonjour-gw-query-forwarding-policy) commands:
  forward-bonjour-query  Forwards bonjour query across vlans
  no                     Negate a command or set its defaults
  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-bonjour-gw-query-forwarding-policy-test)#

Related Commands
- no  Removes an existing Bonjour GW Query Forwarding policy

Note: In the Bonjour GW Query Forwarding policy configuration mode, specify the ‘from’ and ‘to’ VLAN(s). The from-vlans option configures the VLAN(s) that are the source of the Bonjour queries. The to-vlans option configures the destination VLAN(s) that can access the Bonjour queries.

Note: To associate a Bonjour GW Query Forwarding policy with a device or profile, in the profile/device configuration mode, execute the use > bonjour-gw-query-forwarding-policy > <POLICY-NAME> command. For more information see, use.
4.1.27 captive portal

Global Configuration Commands

A captive portal provides secure guest access and authentication services within the network. The following table lists the commands available to enter the captive portal configuration mode:

Table 4.6 Captive-Portal Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal</td>
<td>Creates a new captive portal and enters its configuration mode</td>
<td>page 4-68</td>
</tr>
<tr>
<td>captive-portal-mode</td>
<td>Summarizes captive portal configuration commands</td>
<td>page 4-70</td>
</tr>
<tr>
<td>commands</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.27.1 captive-portal

- captive portal

Configures a captive portal

A captive portal provides secure access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Acknowledgment, Agreement, Welcome, No Service, and Fail pages provide the administrator options to customize the screen flow and user appearance.

Captive portals are recommended for providing guests or visitors authenticated access to network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a username and password pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a datacenter.

Captive portals use a Web provisioning tool to create guest user accounts directly on the controller, service platform, or access point. The connection medium defined for the Web connection is either HTTP or HTTPS. Both HTTP and HTTPS use a request and response procedure to disseminate information to and from requesting wireless clients.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
captive-portal <CAPTIVE-PORTAL-NAME>
```

Parameters

- captive-portal <CAPTIVE-PORTAL-NAME>

Examples

```
rfs7000-37FABE(config)#captive-portal test
rfs7000-37FABE(config-captive-portal-test)#?
```

Captive Portal Mode commands:

- `access-time` Allowed access time for the client. Used when there is no session time in radius response
- `access-type` Access type of this captive portal
- `accounting` Configure how accounting records are created for this captive portal policy
- `bypass` Bypass captive portal
- `connection-mode` Connection mode for this captive portal
- `custom-auth` Custom user information
- `data-limit` Enforce data limit for clients
- `inactivity-timeout` Inactivity timeout in seconds. If a frame is not received from client for this amount of time, then current session will be removed
- `localization` Configure the FQDN address to get the localization parameters for the client
- `ipv6` Internet Protocol version 6 (IPv6)
- `logout-fqdn` Configure the FQDN address to logout the session from client
- `no` Negate a command or set its defaults
- `oauth` OAuth 2.0 authentication configuration
GLOBAL CONFIGURATION COMMANDS 4-69

post-authentication-vlan  Configure post authentication vlan for captive portal users
radius-vlan-assignment    Enable radius vlan assignment for captive portal users
redirection               Configure connection redirection parameters
server                    Configure captive portal server parameters
simultaneous-users        Particular username can only be used by a certain number of MAC addresses at a time
terms-agreement           User needs to agree for terms and conditions
use                       Set setting to use
webpage                   Configure captive portal webpage parameters
webpage-auto-upload       Enable automatic upload of advanced webpages
webpage-location          The location of the webpages to be used for authentication. These pages can either be hosted on the system or on an external web server.
welcome-back             Welcome back page settings
clrscr                    Clears the display screen
commit                    Commit all changes made in this session
do                        Run commands from Exec mode
end                       End current mode and change to EXEC mode
exit                      End current mode and down to previous mode
help                      Description of the interactive help system
revert                    Revert changes
service                   Service Commands
show                      Show running system information
write                     Write running configuration to memory or terminal

rfs7000-37FABE(config-captive-portal-test)#

Related Commands

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an existing captive portal</td>
</tr>
</tbody>
</table>
4.1.27.2 captive-portal-mode commands

The following table summarizes captive portal configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-time</td>
<td>Defines a client’s access time. It is used when no session time is defined in the RADIUS response.</td>
<td>page 4-72</td>
</tr>
<tr>
<td>access-type</td>
<td>Configures a captive portal’s access type</td>
<td>page 4-73</td>
</tr>
<tr>
<td>accounting</td>
<td>Enables a captive portal’s accounting records</td>
<td>page 4-74</td>
</tr>
<tr>
<td>bypass</td>
<td>Enables bypassing of captive portal detection requests from wireless clients</td>
<td>page 4-76</td>
</tr>
<tr>
<td>connection-mode</td>
<td>Configures a captive portal’s connection mode</td>
<td>page 4-77</td>
</tr>
<tr>
<td>custom-auth</td>
<td>Configures custom user information</td>
<td>page 4-78</td>
</tr>
<tr>
<td>data-limit</td>
<td>Enforces data limit on captive portal clients</td>
<td>page 4-79</td>
</tr>
<tr>
<td>inactivity-timeout</td>
<td>Defines an inactivity timeout in seconds</td>
<td>page 4-80</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures the IPv6 address of the internal captive portal server</td>
<td>page 4-81</td>
</tr>
<tr>
<td>localization</td>
<td>Configures an FQDN address string that enables the client to receive localization parameters. This command also allows the configuration of a response message.</td>
<td>page 4-82</td>
</tr>
<tr>
<td>logout-fqdn</td>
<td>Clears the logout FQDN address</td>
<td>page 4-84</td>
</tr>
<tr>
<td>no</td>
<td>Reverts the selected captive portal’s settings to default</td>
<td>page 4-85</td>
</tr>
<tr>
<td>oauth</td>
<td>Enables OAuth-based authentication support on the captive portal. When enabled, OAuth allows captive-portal users to sign in to guest WLANs using their Facebook or Google credentials.</td>
<td>page 4-87</td>
</tr>
<tr>
<td>post-authentication-vlan</td>
<td>Assigns a post authentication RADIUS VLAN for this captive portal’s users</td>
<td>page 4-88</td>
</tr>
<tr>
<td>radius-vlan-assignment</td>
<td>Assigns a RADIUS VLAN for this captive portal</td>
<td>page 4-89</td>
</tr>
<tr>
<td>redirection</td>
<td>Enables redirection of client connections to specified destination ports</td>
<td>page 4-90</td>
</tr>
<tr>
<td>server</td>
<td>Configures the captive portal server settings</td>
<td>page 4-91</td>
</tr>
<tr>
<td>simultaneous-users</td>
<td>Specifies a username used by a MAC address pool</td>
<td>page 4-93</td>
</tr>
<tr>
<td>terms-agreement</td>
<td>Enforces the user to agree to terms and conditions (included in login page) for captive portal access</td>
<td>page 4-94</td>
</tr>
<tr>
<td>use</td>
<td>Associates a AAA policy and a DNS whitelist with a captive portal</td>
<td>page 4-95</td>
</tr>
<tr>
<td>webpage</td>
<td>Configures captive portal Web page settings</td>
<td>page 4-96</td>
</tr>
</tbody>
</table>
Table 4.7 Captive-Portal-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webpage-auto-upload</code></td>
<td>Enables automatic upload of advanced Web pages on a captive portal</td>
<td>page 4-104</td>
</tr>
<tr>
<td><code>webpage-location</code></td>
<td>Specifies the location of Web pages used for captive portal authentication</td>
<td>page 4-105</td>
</tr>
<tr>
<td><code>welcome-back</code></td>
<td>Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins</td>
<td>page 4-106</td>
</tr>
</tbody>
</table>
4.1.27.2.1 access-time

* captive-portal-mode commands

Defines the permitted access time for a client. It is used when no session time is defined in the RADIUS response.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

access-time <10-10080>

Parameters

- access-time <10-10080>

<table>
<thead>
<tr>
<th>access-time &lt;10-10080&gt;</th>
<th>Defines the duration wireless clients are allowed access to the Internet using this captive portal policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;10-10080&gt; – Specify a value from 10 - 10080 minutes. The default is 1440 minutes.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-captive-portal-test)#access-time 35
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
access-time 35
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

- no
  Reverts to the default permitted access time (1440 minutes)
4.1.27.2.2 **access-type**

* captive-portal-mode commands

Defines the captive portal's access type. The authentication scheme configured here is applied to wireless clients using this captive portal.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
access-type [custom-auth-radius|logging|no-auth|radius|registration]
```

**Parameters**

- **access-type [custom-auth-radius|logging|no-auth|radius|registration]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom-auth-radius</td>
<td>Specifies the custom user information used for authentication (RADIUS lookup of given information, such as name, e-mail address, telephone etc.). When configured, accessing clients are required to provide a 1-32 character lookup data string used to authenticate their credentials. <strong>Note:</strong> When selecting this option, use the custom-auth command to configure the required user information.</td>
</tr>
<tr>
<td>logging</td>
<td>Provides users access without authentication. The system logs access details of users allowed access.</td>
</tr>
<tr>
<td>no-auth</td>
<td>Defines no authentication required for a guest (guest is redirected to welcome message). Provides users access to the captive portal without authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Enables RADIUS authentication for wireless clients. Provides captive portal access to successfully authenticated users only. This is the default setting.</td>
</tr>
<tr>
<td>registration</td>
<td>Enables captive portal's clients to self register in the captive portal's database <strong>Note:</strong> If enabled, use the <code>webpage &gt; internal &gt; registration &gt; field</code> command to customize the registration page. If not customized, the default, built-in registration Web page is displayed.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-captive-portal-test)#access-type logging
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
  access-type logging
  access-time 35
rfs7000-37FABE(config-captive-portal-test)#
```

**Related Commands**

```
no
```

Removes the captive portal access type or reverts to default (radius)
4.27.2.3 accounting

captive-portal-mode commands

Enables support for accounting messages for this captive portal

When enabled, accounting for clients entering and exiting the captive portal is initiated. Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data. This data includes information, such as start and stop times, executed commands (such as PPP), number of packets and number of bytes transmitted etc. Accounting enables tracking of captive portal services consumed by clients.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

accounting [radius|syslog]

accounting radius

accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}

Parameters

- accounting radius

  radius Enables support for RADIUS accounting messages. When enabled, this option uses an external RADIUS resource for AAA accounting. This option is disabled by default.

  • accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}

- syslog host <IP/HOSTNAME>

  Enables support for syslog accounting messages. When enabled, data relating to wireless client usage of remote access services is logged on the specified external syslog resource. This information assists in differentiating between local and remote users. Remote user information can be archived to an external location for periodic network and user administration. This option is disabled by default.

  - host <IP/HOSTNAME> — Specifies the destination where accounting messages are sent. Specify the destination’s IP address or hostname.

  port <1-65535> Optional. Specifies the syslog server’s listener port

  - <1-65535> – Specify the UDP port from 1-65535. The default is 514.

  proxy-mode [none|through-controller|through-rf-domain-manager] Optional. Specifies the mode of proxying the syslog server

  - none – Accounting messages are sent directly to the syslog server
  - through-controller – Accounting messages are sent through the controller configuring the device
  - through-rf-domain-manager – Accounting messages are sent through the local RF Domain manager
Examples
rfs7000-37FABE(config-captive-portal-test)#accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
   access-type logging
   access-time 35
   accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables accounting records for this captive portal</td>
</tr>
</tbody>
</table>
4.1.27.2.4 bypass

* captive-portal-mode commands

Enables bypassing of captive portal detection requests from wireless clients

Certain devices, such as Apple IOS devices send Captive Network Assistant (CNA) requests to detect existence of captive portals. When enabled, the bypass option does not allow CNA requests to be redirected to the captive portal pages.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

bypass captive-portal-detection

Parameters

- bypass captive-portal-detection

| bypass captive-portal-detection | Bypasses captive portal detection requests |

Examples

rfs4000-229D58(config-captive-portal-test)#bypass captive-portal-detection
rfs4000-229D58(config-captive-portal-test)#show context captive-portal test
  bypass captive-portal-detection
rfs4000-229D58(config-captive-portal-test)#

Related Commands

- no | Disables bypassing of captive portal detection requests |
4.1.27.2.5 connection-mode

**captive-portal-mode commands**

Configures a captive portal’s mode of connection to the Web server. HTTP uses plain unsecured connection for user requests. HTTPS uses an encrypted connection to support user requests.

Both HTTP and HTTPS use the same *Uniform Resource Identifier* (URI), so controller and client resources can be identified. However, the use of HTTPS is recommended, as it affords controller and client transmissions some measure of data protection HTTP cannot provide.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`connection-mode [http|https]`

**Parameters**

- `connection-mode [http|https]`

<table>
<thead>
<tr>
<th>http</th>
<th>Sets HTTP as the default connection mode. This is the default setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>https</td>
<td>Sets HTTPS as the default connection mode</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-captive-portal-test)#connection-mode https
rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
  access-type logging
  access-time 35
  connection-mode https
  accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#
```

**Related Commands**

- `no` Removes this captive portal’s connection mode
4.1.27.2.6 custom-auth

captive-portal-mode commands

Configures custom user information

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

custom-auth info <LINE>

Parameters

- custom-auth info <LINE>

| info <LINE> | Configures information used for RADIUS lookup when custom-auth RADIUS access type is configured
|            | • <LINE> – Guest data needs to be provided. Specify the name, e-mail address, and telephone number of the user.

Examples

rfs7000-37FABE(config-captive-portal-test)#custom-auth info bob bob@examplecompany.com

rfs7000-37FABE(config-captive-portal-test)#show context
  captive-portal test
  access-type logging
  access-time 35
  custom-auth info bob bob@examplecompany.com
  connection-mode https
  accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

- no
  Removes custom user information configured with this captive portal
4.27.2.7 data-limit

> captive-portal-mode commands

Enforces data transfer limits on captive portal clients. This feature enables the tracking and logging of user usage. Users exceeding the allowed bandwidth are restricted from the captive portal.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

data-limit <1-102400> {action [log-and-disconnect|log-only]}

Parameters
- data-limit <1-102400> {action [log-and-disconnect|log-only]}

<table>
<thead>
<tr>
<th>data-limit &lt;1-102400&gt;</th>
<th>Sets a captive portal client’s data transfer limit in megabytes. This limit is applicable for both upstream and downstream data transfer.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-102400&gt; – Specify a value from 1 - 102400 MB.</td>
</tr>
</tbody>
</table>

| action [log-and-disconnect|log-only] | Optional. Specifies the action taken when a client exceeds the configured data limit. The options are: |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------|
|                                        | • log-and-disconnect – Logs a record and disconnects the client                                        |
|                                        | • log-only – Only a log is generated and the client remains connected to the captive portal. This is the default setting. |

Examples

rfs7000-37FABE(config-captive-portal-test)#data-limit 200 action log-and-disconnect

rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
data-limit 200 action log-and-disconnect
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

| no | Removes data limit enforcement for captive portal clients |
4.27.2.8 inactivity-timeout

Defines an inactivity timeout in seconds. If a frame is not received from a client for the specified interval the current session is terminated.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
inactivity-timeout <60-86400>

Parameters
- inactivity-timeout <60-86400>

<table>
<thead>
<tr>
<th>&lt;60-86400&gt;</th>
<th>Defines the timeout interval after which a captive portal session is automatically terminated</th>
</tr>
</thead>
<tbody>
<tr>
<td>- &lt;60-86400&gt;</td>
<td>Specify a value from 60 - 86400 seconds. The default is 10 minutes or 600 seconds.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-captive-portal-test)#inactivity-timeout 750
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
access-type logging
access-time 35
custom-auth info bob bob@examplecompany.com
custom-auth info bob bob@examplecompany.com
connection-mode https
inactivity-timeout 750
accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#

Related Commands
- **no** Removes the client inactivity interval configured with this captive portal
4.1.27.2.9 ipv6

`captive-portal-mode commands`

Configures the internal captive portal server's (running on the centralized mode) IPv6 address. If using centralized server mode, use this option to define the controller, service platform, or access point resource's (hosting the captive portal) IPv6 address. For information on configuring the server mode, see `server`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ipv6 server host <IPv6>`

**Parameters**

- `ipv6 server host <IPv6>`

<table>
<thead>
<tr>
<th><code>ipv6 server host &lt;IPv6&gt;</code></th>
<th>Configures the IPv6 address of the internal captive portal server</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv6&gt;</code></td>
<td><code>&lt;IPv6&gt;</code> – Specify the captive portal server’s global IPv6 address.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-6DCD4B(config-captive-portal-test2)#show context captive-portal test2 access-type OAuth
rfs7000-6DCD4B(config-captive-portal-test2)#

**Related Commands**

`no` Removes the captive portal server’s IPv6 address
4.1.27.2.10 localization

* captive-portal-mode commands

Configures an FQDN address string that enables the client to receive localization parameters. Use this option to add a URL to trigger a one-time redirect on demand. The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
localization [fqdn <WORD>|response <WORD>]
```

**Parameters**

- **localization [fqdn <WORD>|response <WORD>]**

  - **fqdn <WORD>**: Configures the FQDN address string, which is used to obtain localization parameters for the captive portal's client.
    - `<WORD>` – Specify the FQDN address string. For example, local.guestaccess.com

  - **response <WORD>**: Configures a message, which is sent back to the client in response to the client’s localization HTTP requests.
    - `<WORD>` – Specify the response message (should not exceed 512 characters in length). The following built-in query tags can be included in the response message:
      - `WING_TAG_CLIENT_IP` - Captive portal client IPv4 address
      - `WING_TAG_CLIENT_MAC` - Captive portal client MAC address
      - `WING_TAG_WLAN_SSID` - Captive portal client WLAN ssid
      - `WING_TAG_AP_MAC` - Captive portal client AP MAC address
      - `WING_TAG_AP_NAME` - Captive portal client AP Name
      - `WING_TAG_RF_DOMAIN` - Captive portal client RF Domain
      - `WING_TAG_USERNAME` - Captive portal authentication username
      - `WING_TAG_USERTYPE` - Captive portal usertype
      - `(new/return/refresh)`
      - Example:-
        ```
        <local><site>WING_TAG_RF_DOMAIN</site><ap>WING_TAG_AP_NAME</ap></local>
        ```

**Examples**

```
nx4500-5CFA2B(config-captive-portal-test)#localization fqdn local.guestaccess.com

nx4500-5CFA2B(config-captive-portal-test)#localization response <local><site>SJZebra</site><ap>ap8132-74B45C</ap><user>Bob</user></local>

nx4500-5CFA2B(config-captive-portal-test)#show context include-factory | include localization
localization fqdn local.guestaccess.com
localization response <local><site>SJZebra</site><ap>ap8132-74B45C</ap><user>Bob</user></local>
```

nx4500-5CFA2B(config-captive-portal-test)#
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the FQDN address string and response message configured on a captive portal for localization</td>
</tr>
</tbody>
</table>
4.1.27.2.11 logout-fqdn

Configure captive-portal-mode commands

Configure the Fully Qualified Domain Name (FQDN) address to logout of the session from the client.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

logout-fqdn <WORD>

Parameters

- logout-fqdn <WORD>

Examples

rfs7000-37FABE(config-captive-portal-test)#logout-fqdn logout.testuser.com

Related Commands

- no
  - Clears the logout FQDN address
4.1.27.2.12  no

**captive-portal-mode commands**

The `no` command reverts the selected captive portal’s settings or resets settings to default.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [access-time|access-type|accounting|bypass|connection-mode|custom-auth|data-limit|
inactivity-timeout|ipv6|localization|logout-fqdn|oauth|post-authentication-vlan|
radius-vlan-assignment|redirection|serversimultaneous-users|terms-agreement|use|
webpage|webpage-auto-upload|webpage-location|welcome-back]

no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|logout-fqdn|
post-authentication-vlan|radius-vlan-assignment|simultaneous-users|terms-agreement|
webpage-auto-upload|webpage-location]

no accounting [radius|syslog]
no bypass captive-portal-detection
no custom-auth info
no ipv6 server host
no localization [fqdn|response]
no oauth {client-id}
no redirection ports
no server host
no server mode {centralized-controller [hosting-vlan-interface]}
no use [aaa-policy|dns-whitelist]
no webpage external [acknowledgment|agreement|fail|login {post}|no-service|
registration|welcome]

no webpage internal [acknowledgment|agreement|fail|login|no-service|org-name|
org-signature|registration|welcome]
no webpage internal [org-name|org-signature]
no webpage internal [acknowledgment|agreement|fail|login|no-service]
[body-background-color|body-font-color|description|footer|header|main-logo|
org-background-color|org-font-color|small-logo|title]
no webpage internal registration [body-background-color|body-font-color|description|
field|footer|header|main-logo|org-background-color|org-font-color|small-logo|title]
no webpage internal registration field [age-range|city|country|custom <FIELD-NAME>|
disclaimer|dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip|
enable]

no webpage internal welcome [body-background-color|body-font-color|description|
footer|header|main-logo|org-background-color|org-font-color|small-logo|title|
use-external-success-url]
no welcome-back pass-through
```
Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes or resets this captive portal's settings, based on the parameters passed. |

Examples

The following example shows the captive portal 'test' settings before the 'no' commands are executed:

```
  rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
  access-type logging
  access-time 35
  custom-auth info bob bob@examplecompany.com
  connection-mode https
  inactivity-timeout 750
  accounting syslog host 172.16.10.13 port 1
  rfs7000-37FABE(config-captive-portal-test)#
```

```
  rfs7000-37FABE(config-captive-portal-test)#no accounting syslog
  rfs7000-37FABE(config-captive-portal-test)#no access-type
```

The following example shows the captive portal 'test' settings after the 'no' commands are executed:

```
  rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
  access-time 35
  custom-auth info bob bob@examplecompany.com
  connection-mode https
  inactivity-timeout 750
  rfs7000-37FABE(config-captive-portal-test)#
```
4.27.2.13 oauth

Enables OAuth-based authentication support on this captive portal. When enabled, OAuth allows captive-portal users to sign in to guest WLANs using their Facebook or Google credentials.

OAuth is an open-source protocol that allows secure authorization from Web, mobile, and desktop applications. The OAuth 2.0 authorization framework enables a third-party application (which, in this scenario, is the WiNG software) to obtain limited access to an HTTP service. The WiNG software running on an access point or a controller provides the captive portal authentication service. Wireless clients accessing a guest WLAN using OAuth are asked for their Google or Facebook credentials, and are allowed network access only upon successful authentication.

Supported in the following platforms:
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

oauth {client-id [facebook|google] <WORD>}

Parameters

- oauth {client-id [facebook|google] <WORD>}

<table>
<thead>
<tr>
<th>oauth</th>
<th>Configures OAuth 2.0 settings required to provide OAuth access to clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-id [facebook</td>
<td>google] &lt;WORD&gt;</td>
</tr>
<tr>
<td>facebook – Configures the client's Facebook ID</td>
<td></td>
</tr>
<tr>
<td>google – Configures the client's Google ID</td>
<td></td>
</tr>
<tr>
<td>&lt;WORD&gt; – Provide the client's Facebook/Google ID (should be registered with the OAuth provider)</td>
<td></td>
</tr>
</tbody>
</table>

Examples

rfs7000-6DCD4B(config-captive-portal-test2)#OAuth client-id Google TechPubs.printer.google.com
rfs7000-6DCD4B(config-captive-portal-test2)#show context captive-portal test2  
OAuth client-id Google TechPubs.printer.google.com  
rfs7000-6DCD4B(config-captive-portal-test2)#

Related Commands

- no | Removes all OAuth client identities configured for this captive portal |
4.1.27.2.14 post-authentication-vlan

**captive-portal-mode commands**

Configures the VLAN that is assigned to this captive portal’s users upon successful authentication.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]`

**Parameters**

- `post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]`

| post-authentication-vlan [<1-4096>|<VLAN-ALIAS>] | Configures the post authentication VLAN. The VLAN specified here is assigned to this captive portal’s users after they have authenticated and logged on to the network. Provide the VLAN ID, or use an existing VLAN alias to identify the post authentication VLAN. |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                                               | • <1-4096> – Specify the VLAN’s number from 1 - 4096. |
|                                               | • <VLAN-ALIAS> – Specify the VLAN alias (should be existing and configured). |

**Note:** VLAN alias names begin with a ‘$’.

**Examples**

```
rfs4000-229D58(config-captive-portal-test)#post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#show context captive-portal test
post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the post authentication RADIUS VLAN assigned to this captive portal’s users</td>
</tr>
<tr>
<td><strong>radius-vlan-assignment</strong></td>
<td>Enables assignment of a RADIUS VLAN for this captive portal</td>
</tr>
</tbody>
</table>
4.1.27.2.15 radius-vlan-assignment

Enables assignment of a RADIUS VLAN for this captive portal

When enabled, if the RADIUS server as part of the authentication process returns a client's VLAN-ID in a RADIUS access-accept packet, then all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

radius-vlan-assignment

Parameters

None

Examples

rfs4000-229D58(config-captive-portal-test)#radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#show context captive-portal test
post-authentication-vlan 1
radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables assignment of a RADIUS VLAN for this captive portal</td>
</tr>
<tr>
<td>post-authentication-vlan</td>
<td>Assigns a post authentication RADIUS VLAN for this captive portal's users</td>
</tr>
</tbody>
</table>
4.1.27.2.16 redirection

- captive-portal-mode commands

Configures a list of destination ports (separated by commas, or using a dash for a range) that are taken into consideration when redirecting client connections.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

redirection ports <LIST-OF-PORTS>

Parameters

- redirection ports <LIST-OF-PORTS>

<table>
<thead>
<tr>
<th>ports &lt;LIST-OF-PORTS&gt;</th>
<th>Configures destination ports considered for redirecting client connection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> A maximum of 16 ports can be specified in a comma-separated list. Standard ports 80 and 443 are always considered for client connections regardless of what's entered by the administrator.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-captive-portal-test)#redirection ports 1,2,3
rfs4000-229D58(config-captive-portal-test)#show context captive-portal test redirection ports 1-3
rfs4000-229D58(config-captive-portal-test)#

Related Commands

| no | Disables redirection of client connection |
4.1.27.2.17 server

* captive-portal-mode commands

Configures captive portal server parameters, such as the hostname, IP address, and mode of operation. This is the server validating guest user permissions.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
server [host|mode]
server host <IP/HOSTNAME>
server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]
```

**Parameters**
- **host <IP/HOSTNAME>**
  
  Configures the internal captive portal authentication server (wireless controller, access point, service platform)

  - `<IP/HOSTNAME>` – Specify the IPv4 address or hostname of the captive portal server.

  **Note:** For centralized wireless controller mode, this should be a virtual hostname and not an IP address.

  **Note:** This option is available only when hosting the captive portal on an external (fixed) server resource.

- **server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]**

<table>
<thead>
<tr>
<th>mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>centralized</td>
<td>Considers the configured server’s hostname or IP address as the centralized captive portal server. Select this option if the captive portal is supported on an external server.</td>
</tr>
<tr>
<td>centralized-controller {hosting-vlan-interface &lt;0-4096&gt;}</td>
<td>Configures the numeric IP address (or DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is available only for the centralized (external) AND centralized-controller captive portal server resources.</td>
</tr>
<tr>
<td></td>
<td>• hosting-vlan-interface – Optional. Configures the VLAN where the client can reach the wireless controller (server). This option is available only for the centralized-controller mode.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;0-4096&gt;</code> – Specify the VLAN number (0 implies the controller is available on the client’s VLAN).</td>
</tr>
<tr>
<td>self</td>
<td>Selects the captive portal server as the same device supporting the WLAN (the captive portal and the WLAN are configured on the same device). Select this option to maintain the captive portal configuration (Web pages) internally. This is the default setting.</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-captive-portal-test)#server host 172.16.10.9

rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
access-time 35
       custom-auth info bob bob@examplecompany.com
   connection-mode https
    inactivity-timeout 750
   server host 172.16.10.9
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

| no | Resets or disables captive portal host and mode settings |
4.27.18 simultaneous-users

**captive-portal-mode commands**

Specifies the number of users (client MAC addresses) that can simultaneously logon to the captive portal. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

simultaneous-users <1-8192>

**Parameters**

- simultaneous-users <1-8192>

<table>
<thead>
<tr>
<th>simultaneous-users &lt;1-8192&gt;</th>
<th>Specifies the number of MAC addresses that can simultaneously access the captive portal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-8192&gt; – Select a number from 1 - 8192.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-captive-portal-test)#simultaneous-users 5

rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
access-time 35
custom-auth info bob bob@examplecompany.com
collection-mode https
inactivity-timeout 750
server host 172.16.10.9
simultaneous-users 5
rfs7000-37FABE(config-captive-portal-test)#

**Related Commands**

- **no** | Resets or disables captive portal commands
4.1.27.2.19 terms-agreement

➤ captive-portal-mode commands

Enforces the user to agree to terms and conditions (included in the login page) for captive portal access. This feature is disabled by default.

When enabled, the system enforces a previously registered user to re-confirm the terms of agreement, on successive log ins, only if the interval between the last log out and the current log in exceeds the agreement-refresh timeout configured in the WLAN context. For more information on configuring the agreement-refresh timeout value, see registration.

For example:

If the agreement-refresh timeout is set at 20 minutes, the following two possibilities can arise:

• The interval between logging out and re-logging exceeds 20 minutes - in which case the user is served the Terms of Agreement page on successful authentication.
• The interval between logging out and re-logging is less than 20 minutes - in which case the user is provided direct Internet access.

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9600

Syntax
terms-agreement

Parameters
None

Examples
rfs7000-37FABE(config-captive-portal-test)#terms-agreement
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
  access-time 35
custom-auth info bob bob@examplecompany.com
connection-mode https
inactivity-timeout 750
server host 172.16.10.9
simultaneous-users 5
terms-agreement
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets or disables captive portal commands</td>
</tr>
</tbody>
</table>
4.27.2.20 use

> captive-portal-mode commands

Configures a AAA policy and DNS whitelist with this captive portal policy. AAA policies are used to configure authentication and accounting servers for this captive portal. DNS whitelists restrict users to a set of configurable domains on the Internet.

For more information on AAA policies, see Chapter 8, AAA-POLICY.

For more information on DNS whitelists, see Chapter 4, dns-whitelist.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

text

Parameters

- use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]

Examples

rfs7000-37FABE(config-captive-portal-test)# use aaa-policy test
rfs7000-37FABE(config-captive-portal-test)# use dns-whitelist test
rfs7000-37FABE(config-captive-portal-test)#show context
captive-portal test
  access-time 35
custom-auth info bob bob@examplecompany.com
collection-mode https
inactivity-timeout 750
server host 172.16.10.9
simultaneous-users 5
terms-agreement
  use aaa-policy test
  use dns-whitelist test
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes a DNS Whitelist or a AAA policy from the captive portal</td>
</tr>
<tr>
<td>dns-whitelist</td>
<td>Configures a DNS whitelist</td>
</tr>
<tr>
<td>aaa-policy</td>
<td>Configures a AAA policy</td>
</tr>
</tbody>
</table>
4.1.27.2.21 webpage

Use this command to define the appearance and flow of Web pages requesting clients encounter when accessing a controller, service platform, or access point managed captive portal. Define whether the Web pages are maintained locally or externally to the managing device as well as messages displayed requesting clients.

Configures Web pages displayed when interacting with a captive portal. These pages are:

- acknowledgment – This page displays details for the user to acknowledge
- agreement – This page displays "Terms and Conditions" that a user accepts before allowed access to the captive portal.
- fail – This page is displayed when the user is not authenticated.
- login – This page is displayed when the user connects to the captive portal. It fetches login credentials from the user.
- no-service – This page is displayed when a captive portal user is unable to access the captive portal due to unavailability of critical services.
- registration – This page is displayed when users are redirected to a Web page where they have to register in the captive portal's database.
- welcome – This page is displayed to welcome an authenticated user to the captive portal.

These Web pages, which interact with captive portal users, can be located either on the controller or an external location.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NXT9510, NX9600

Syntax

webpage [external|internal]

webpage external [acknowledgment|agreement|fail|login {post}|no-service|registration|welcome] <URL>

webpage internal [acknowledgment|agreement|fail|login|no-service|org-name|org-signature|registration|welcome]

description|footer|header|title <CONTENT>

webpage internal registration field [age-range|city|country|custom|disclaimer|dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip] type [checkbox|date|dropdown-menu|e-address|number|radio-button|text] enable {label <LINE>|mandatory|title <LINE>|placeholder <LINE>}

webpage internal welcome use-external-success-url

webpage internal [org-name|org-signature] <LINE>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webpage external</code> [acknowledgment</td>
<td>agreement</td>
</tr>
<tr>
<td><code>external</code></td>
<td>Indicates the page is displayed for user acknowledgment of details. Users are redirected to this page to acknowledge information provided.</td>
</tr>
<tr>
<td><code>acknowledgment</code></td>
<td>Indicates the page is displayed for “Terms &amp; Conditions” The agreement page provides conditions that must be agreed to before captive portal access is permitted.</td>
</tr>
<tr>
<td><code>agreement</code></td>
<td>Indicates the page is displayed for login failure The fail page asserts authentication attempt has failed, the user is not allowed to access the Internet (using this captive portal) and must provide the correct login information again to access the Internet.</td>
</tr>
<tr>
<td><code>fail</code></td>
<td>Indicates the page is displayed for getting user credentials. This page is displayed by default.</td>
</tr>
<tr>
<td><code>login {post}</code></td>
<td>Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The no-service page asserts the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal. The possible scenarios are:</td>
</tr>
<tr>
<td><code>no-service</code></td>
<td>To provide this service, enable the following:</td>
</tr>
<tr>
<td><code>registration</code></td>
<td>Indicates the page is displayed when users are redirected to a Web page where they have to register in the captive portal’s database. Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.</td>
</tr>
<tr>
<td><code>welcome</code></td>
<td>Indicates the page is displayed after a user has been successfully authenticated. The welcome page asserts a user has logged in successfully and can access the captive portal.</td>
</tr>
</tbody>
</table>
### <URL>

This parameter is common to all of the above mentioned Web pages, and specifies the Web page URL. The Web page is retrieved and served from the specified external location.

The URL can include following query tags:

- `WING_TAG_CLIENT_IP` - Captive portal client IPv4 address
- `WING_TAG_CLIENT_MAC` - Captive portal client MAC address
- `WING_TAG_WLAN_SSID` - Captive portal client WLAN ssid
- `WING_TAG_AP_MAC` - Captive portal client AP MAC address
- `WING_TAG_AP_NAME` - Captive portal client AP Name
- `WING_TAG_RF_DOMAIN` - Captive portal client RF Domain
- `WING_TAG_CP_SERVER` - Captive portal server address
- `WING_TAG_USERNAME` - Captive portal authentication username

Example:

```
http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&ap_m
```

Use `&` or `?` character to separate field-value pair.

**Note:** Enter ‘ctrl-v’ followed by ‘?’ to configure query string.

### webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome] [description|footer|header|title] <CONTENT>

<table>
<thead>
<tr>
<th>internal</th>
<th>Indicates the Web pages are hosted on an internal server resource. This is the default setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>acknowledgment</td>
<td>Indicates the Web page is displayed for users to acknowledge the information provided</td>
</tr>
<tr>
<td>agreement</td>
<td>Indicates the page is displayed for “Terms &amp; Conditions”</td>
</tr>
<tr>
<td>fail</td>
<td>Indicates the page is displayed for login failure</td>
</tr>
<tr>
<td>login</td>
<td>Indicates the page is displayed for entering user credentials</td>
</tr>
<tr>
<td>no-service</td>
<td>Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are:</td>
</tr>
<tr>
<td>registration</td>
<td>Indicates the page is displayed when users are redirected to a Web page where they have to register in the captive portal's database</td>
</tr>
<tr>
<td>welcome</td>
<td>Indicates the page is displayed after a user has been successfully authenticated</td>
</tr>
</tbody>
</table>

*Note:* For more information on enabling these critical resource monitoring, see [service](#).

```python
for more information on enabling these critical resource monitoring, see [service](#).
```
<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates the content is the description portion of each of the following internal Web pages: acknowledgment, agreement, fail, login, no-service, and welcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Footer</td>
<td>Indicates the content is the footer portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The footer portion contains the signature of the organization that hosts the captive portal.</td>
</tr>
<tr>
<td>Header</td>
<td>Indicates the content is the header portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The header portion contains the heading information for each of these pages.</td>
</tr>
<tr>
<td>Title</td>
<td>Indicates the content is the title of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The title for each of these pages is configured here.</td>
</tr>
</tbody>
</table>
| <CONTENT>   | The following keyword is common to all of the above internal Web page options:  
  - <CONTENT> – Specify the content displayed for each of the different components of the internal Web page. Enter up to 900 characters for the description and 256 characters each for header, footer, and title. |

- **webpage internal** [acknowledgment|agreement|fail|login|no-service|registration|welcome] [main-logo use-as-banner|small-logo] <URL>

<table>
<thead>
<tr>
<th>Internal</th>
<th>Indicates the Web pages are hosted on an internal server resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Indicates the page is displayed for “Terms &amp; Conditions”</td>
</tr>
<tr>
<td>Acknowledgment</td>
<td>Indicates the Web page is displayed for users to acknowledge the information provided</td>
</tr>
<tr>
<td>Fail</td>
<td>Indicates the page is displayed for login failure</td>
</tr>
<tr>
<td>Login</td>
<td>Indicates the page is displayed for user credentials</td>
</tr>
</tbody>
</table>
| No-Service  | Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are:  
  - The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated  
  - The external captive portal server is not reachable  
  - The connectivity between the adopted AP and controller is lost  
  - The external DHCP server is not reachable  
  
  To provide this service, enable the following:  
  - External captive portal server monitoring  
  - AAA server monitoring. This enables detection of RADIUS server failure.  
  - External DHCP server monitoring  
  - AP to controller connectivity monitoring  
  
  **Note:** For more information on enabling these critical resource monitoring, see wlan. |
| Registration | Indicates the page displayed is the registration page to which users are redirected in order to register in the captive portal’s database  
  
  Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register. |
<p>| Welcome     | Indicates the page is displayed after a user has been successfully authenticated |</p>
<table>
<thead>
<tr>
<th><strong>main-logo</strong></th>
<th>The following keyword is common to all of the above internal Web page options:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>use-as-banner</strong></td>
<td>• main-logo – Indicates the main logo displayed in the header of each Web page</td>
</tr>
<tr>
<td></td>
<td>• use-as-banner – Uses the image, specified here, as the Web page banner, in place of the logo and organization name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>small-logo</strong></th>
<th>The following keyword is common to all of the above internal Web page options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• small-logo – Indicates the logo image displayed in the footer of each Web page, and constitutes the organization’s signature</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>&lt;URL&gt;</strong></th>
<th>This parameter is common to the ‘main-logo’ and ‘small-logo’ keywords and provides the complete URL from where the main-logo and small-logo files are loaded and subsequently cached on the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;URL&gt; – Specify the location and name of the main-logo and the small-logo image files.</td>
</tr>
</tbody>
</table>

- **webpage internal registration field** [age-range|city|country|custom|disclaimer|dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip] type [checkbox|date|dropdown-menu|e-address|number|radio-button|text] enable {label <LINE>|mandatory|title <LINE>|placeholder <LINE>}

<table>
<thead>
<tr>
<th><strong>internal</strong></th>
<th>Indicates the Web pages are hosted on an internal server resource</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>registration</strong></td>
<td>Allows you to customize the user registration page. Select this option if the captive-portal’s access-type is set to registration. Use the <strong>field</strong> and <strong>type</strong> options to define the input fields (for example, age-range, city, email etc.) and the field type (for example, text, checkbox, dropdown-menu, or radio-button etc.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.</td>
</tr>
<tr>
<td></td>
<td>If the registration Web page is not customized, the built-in, default registration page is displayed to the client.</td>
</tr>
</tbody>
</table>

| **field** [age-range|city|country|custom <WORD>|disclaimer]] | Configures the captive portal’s registration page fields |
|-----------------------------------------------|---------------------------------------------------------|
| **field** [age-range|city|country|custom <WORD>|disclaimer]] | Following are the available fields and the field type for each: |
| | • age-range – Creates the age-range input field (enabled by default and included in the built-in registration page) |
| | • dropdown-menu – Configures the age-range field as a drop-down menu |
| | • radio-button – Configures the age-range field as a radio button menu |
| | • city – Creates the **postal address: city name** input field (enabled by default and included in the built-in registration page) |
| | • text – Configures the city field as only alpha-numeric and special characters input field |
| | • country – Creates the **postal address: country name** input field (disabled by default) |
| | • text – Configures the country field as only alpha-numeric and special characters input field |
| | • custom <WORD> – Creates a customized field (as per your requirement). Use the ‘custom’ option to create a field not included in the built-in list. |
| | • <WORD> – Provide a name for the field. On the registration page, the field is displayed under the name specified here. |
| | • disclaimer – Creates client’s disclaimer-confirmation input field (disabled by default) |
| | • checkbox – Configures the disclaimer field as a check box |

Contd..
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dob</td>
<td>Creates the client’s <em>date of birth</em> (DoB) input field (disabled by default)</td>
</tr>
<tr>
<td>date</td>
<td>Configures the DoB field as only date-format input field</td>
</tr>
<tr>
<td>dropdown-menu</td>
<td>Configures the DoB field as a drop-down menu</td>
</tr>
<tr>
<td>text</td>
<td>Configures the DoB field as only alpha-numeric and special characters input field</td>
</tr>
<tr>
<td>email</td>
<td>Creates the e-mail address input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>e-address</td>
<td>Configures the e-mail field as only e-mail address format input field</td>
</tr>
<tr>
<td>gender</td>
<td>Creates client’s gender input field (disabled by default)</td>
</tr>
<tr>
<td>dropdown-menu</td>
<td>Configures the gender field as a drop-down menu</td>
</tr>
<tr>
<td>radio-button</td>
<td>Configures the gender field as a radio button menu</td>
</tr>
<tr>
<td>member</td>
<td>Creates client’s loyalty or captive-portal membership card number input field (disabled by default)</td>
</tr>
<tr>
<td>number</td>
<td>Configures the member field as only-numeric characters input field</td>
</tr>
<tr>
<td>text</td>
<td>Configures the member field as only alpha-numeric and special characters input field</td>
</tr>
<tr>
<td>mobile</td>
<td>Creates the mobile number input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>number</td>
<td>Configures the mobile field as only-numeric characters input field</td>
</tr>
<tr>
<td>text</td>
<td>Configures the mobile field as only alpha-numeric and special characters input field</td>
</tr>
<tr>
<td>name</td>
<td>Creates the client name input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>text</td>
<td>Configures the name field as only alpha-numeric and special characters input field</td>
</tr>
<tr>
<td>optout</td>
<td>Creates an input field that enables clients to opt out from registering</td>
</tr>
<tr>
<td>checkbox</td>
<td>Configures the optout field as a check box</td>
</tr>
<tr>
<td>street</td>
<td>Creates the <em>postal address: street name/number</em> input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>text</td>
<td>Configures the street field as only alpha-numeric and special characters input field</td>
</tr>
<tr>
<td>via-email</td>
<td>Creates the client’s preferred mode of communication as e-mail input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>checkbox</td>
<td>Configures the via-email field as a check box</td>
</tr>
<tr>
<td>via-sms</td>
<td>Creates the client’s preferred mode of communication as SMS input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>checkbox</td>
<td>Configures the via-sms field as a check box</td>
</tr>
<tr>
<td>zip</td>
<td>Creates the <em>postal address: zip</em> input field (enabled by default and included in the built-in registration page)</td>
</tr>
<tr>
<td>number</td>
<td>Configures the zip field as only-numeric characters input field</td>
</tr>
<tr>
<td>text</td>
<td>Configures the zip field as only alpha-numeric and special characters input field</td>
</tr>
</tbody>
</table>
After specifying the field, configure the field type. The options displayed depend on the field selected in the previous step. These options are: checkbox, date, dropdown-menu, e-address, number, radio-button, and text.

- checkbox – Configures the field as a check box
- date – Configures the field as only date-format input field
- dropdown-menu – Configures the field as a drop-down menu
- e-address – Configures the field as an e-mail address input field
- number – Configures the field as only-numeric characters input field
- radio-button – Configures the field as a radio button
- text – Configures the field as only alpha-numeric and special characters input field

**Note:** Some of the fields can have more than one field type options. For example, the field 'zip' can either be a numerical field or a text. Select the one best suited for your captive-portal.

Enables the field. When enabled, the field is displayed on the registration page. After enabling the field, optionally configure the following parameters:

- label <LINE> – Optional. Configures the field’s label
- mandatory – Optional. Makes the field mandatory
- title – Optional. Configures the comma-separated list of items to include in the drop-down menu.
- placeholder <LINE> – Optional. Configures a string, not exceeding 300 characters, that is displayed within the field. If not configured, the field remains blank.
Examples
rfs6000-81701D(config-captive-portal-guest)#show context captive-portal guest
webpage external welcome http://192.168.9.46/welcome.html
rfs6000-81701D(config-captive-portal-guest)#

nx9500-6C8809(config-captive-portal-register)#webpage internal registration field age-range type dropdown-menu enable mandatory title 10-20,20-30,30-40,50-60,60-70
nx9500-6C8809(config-captive-portal-register)#show context include-factory | include age-range
webpage internal registration field age-range type dropdown-menu enable mandatory label "Age Range" title "10-20,20-30,30-40,50-60,60-70"

In the following examples, the background and font colors have been customized for the captive portal's login page. Similar customizations can be applied to the acknowledgement, agreement, fail, welcome, no-service, and registration captive portal pages.

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login body-background-color #E7F0EB
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login body-font-color #EF68A7
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login org-background-color #EFE4E9
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal login org-font-color #BA4A21
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#show context captive-portal cap-enhanced-policy
webpage internal login org-background-color #EFE4E9
webpage internal login org-font-color #BA4A21
webpage internal login body-background-color #E7F0EB
webpage internal login body-font-color #EF68A7
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#

The following examples configure a scenario where a successfully authenticated user is redirected to an externally hosted Welcome page from the internal landing page.

rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#webpage internal welcome use-external-success-url
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)#show context captive-portal cap-enhanced-policy
webpage internal acknowledgement org-background-color #33ff88
webpage internal acknowledgement org-font-color #bb6622
webpage internal acknowledgement body-background-color #22aa11
webpage internal acknowledgement body-font-color #bb6622
webpage internal welcome use-external-success-url
rfs6000-81701D(config-captive-portal-cap-enhanced-policy)##

Related Commands

| no | Resets or disables captive portal configurations |
4.1.27.2.22 webpage-auto-upload

Enables automatic upload of advanced Web pages to requesting clients on association. Enable this option if the webpage-location is selected as advanced. For more information see, webpage-location.

If this feature is enabled, access points shall request for Web pages from the controller during adoption. If the controller has a different set of Web pages, than the ones existing on the access points, the controller shall distribute the Web pages uploaded on it to the access points.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
webpage-auto-upload

Parameters
None

Examples
rfs7000-37FABE(config-captive-portal-test)#webpage-auto-upload
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test webpage-auto-upload logout-fqdn logout.testuser.com
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables automatic upload of advanced Web pages on a captive portal</td>
</tr>
<tr>
<td>webpage</td>
<td>Configures Web pages displayed when interacting with a captive portal</td>
</tr>
<tr>
<td>webpage-location</td>
<td>Specifies the location of the Web pages used for authentication</td>
</tr>
</tbody>
</table>
### 4.1.27.2.23 webpage-location

**captive-portal-mode commands**

Specifies the location of the Web pages used for authentication. These pages can either be hosted on the system or on an external Web server.

Supported in the following platforms:
- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
webpage-location [advanced|external|internal]
```

#### Parameters

- `webpage-location [advanced|external|internal]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced</td>
<td>Uses Web pages for login, welcome, failure, and terms created and stored on the controller. Select <code>advanced</code> to use a custom-developed directory full of Web page content that can be copied in and out of the controller, service platform, or access point. If selecting advanced, enable the <code>webpage-auto-upload</code> option to automatically launch the advanced pages to requesting clients upon association. For more information, see <code>webpage-auto-upload</code>.</td>
</tr>
<tr>
<td>external</td>
<td>Uses Web pages for login, welcome, failure, and terms located on an external server. Provide the URL for each of these pages.</td>
</tr>
<tr>
<td>internal</td>
<td>Uses Web pages for login, welcome, and failure that are automatically generated</td>
</tr>
</tbody>
</table>

#### Examples

```
rfs7000-37FABE(config-captive-portal-test)#webpage-location external
```

```
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
   access-time 35
   custom-auth info bob bob@examplecompany.com
   connection-mode https
   inactivity-timeout 750
   server host 172.16.10.9
   simultaneous-users 5
   terms-agreement webpage-location external
   use aaa-policy test
rfs7000-37FABE(config-captive-portal-test)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets or disables captive portal Web page settings</td>
</tr>
<tr>
<td><code>webpage</code></td>
<td>Configures a captive portal's Web page (acknowledgment, agreement, login, welcome, fail, no-service, and terms) settings</td>
</tr>
<tr>
<td><code>webpage-auto-upload</code></td>
<td>Enables an automatic upload of advanced Web pages on a captive portal</td>
</tr>
</tbody>
</table>
4.1.27.2.24 welcome-back

► captive-portal-mode commands

Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins. When enabled, a previously registered captive-portal guest user, on subsequent logins, is served the Acknowledgement page only if:

- The agreement-refresh option is enabled for device-based (device and device-OTP) registration, and
- The interval between logout and login is lesser than the agreement-refresh timeout configured in the WLAN context. If this interval exceeds the agreement-refresh timeout, the user is served the Agreement page. For more information on configuring the agreement-refresh timeout value, see registration.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
welcome-back pass-through

Parameters
- welcome-back pass-through

<table>
<thead>
<tr>
<th>welcome-back pass-through</th>
<th>Enables display of the Acknowledgement page to an already registered user on subsequent captive-portal log-ins, provided the interval between logout and login is lesser than the agreement-refresh timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>pass-through</td>
<td>pass-through – Provides user direct Internet access, from the Welcome-back page, without any user action</td>
</tr>
</tbody>
</table>

Examples
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
welcome-back pass-through
webpage internal registration field city type text enable label "City" placeholder "Enter City"
webpage internal registration field street type text enable label "Address" placeholder "123 Any Street"
webpage internal registration field name type text enable label "Full Name" placeholder "Enter First Name, Last Name"
webpage internal registration field zip type number enable label "Zip" placeholder "Zip"
webpage internal registration field via-sms type checkbox enable title "SMS Preferred"
webpage internal registration field mobile type number enable label "Mobile" placeholder "Mobile Number with Country code"
webpage internal registration field age-range type dropdown-menu enable label "Age Range" title "Age Range"
webpage internal registration field email type e-address enable mandatory label "Email" placeholder "you@domain.com"
webpage internal registration field via-email type checkbox enable title "Email Preferred"
nx9500-6C8809(config-captive-portal-test)#

Related Commands

no | Disables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins
4.1.28 clear

Global Configuration Commands

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared using this command varies depending on the mode where executed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

clear event-history

Parameters

- clear event-history

<table>
<thead>
<tr>
<th>event-history</th>
<th>Clears the event history file</th>
</tr>
</thead>
</table>

Examples

rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2015-04-23 16:41:27 IST' by 'admin'

2015-04-23 16:41:21       rfs4000-229D58  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-04-23 16:09:38       rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
'admin' with privilege 'superuser' from '192.168.100.208'
2015-04-23 16:09:29       rfs4000-229D58  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-04-23 11:09:20       rfs4000-229D58  SYSTEM     CONFIG_REVISION      Configuration revision updated to 5 from 4
2015-04-23 11:07:19       rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
'admin' with privilege 'superuser' from '192.168.100.208'
2015-04-23 11:07:19       rfs4000-229D58  SYSTEM     CONFIG_COMMIT        Configuration commit by user 'cfgd' (read startup-config) from '127.0.0.1'
2015-04-23 11:07:19       rfs4000-229D58  LICMGR   LIC_REMOVED   ADSEC license removed

rfs4000-229D58#clear event-history

rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2015-04-23 16:42:24 IST' by 'admin'

rfs4000-229D58#
4.1.29 client-identity

Global Configuration Commands

With an increase in Bring Your Own Device (BYOD) corporate networks, there is a parallel increase in the number of possible attack scenarios within the network. BYOD devices are inherently unsafe, as the organization’s security mechanisms do not extend to these personal devices deployed in the corporate wireless network. Organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting assists administrators by controlling how BYOD devices access a corporate wireless domain. Device fingerprinting uses DHCP options sent by the client in request or discover packets to derive a unique signature specific to device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each device class.

The following table summarizes the commands available for creating and configuring a set of new client identity parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identity</td>
<td>Creates a new client identity and enters its configuration mode</td>
<td>page 4-109</td>
</tr>
<tr>
<td>client-identity-mode</td>
<td>Invokes the client identity policy configuration mode commands</td>
<td>page 4-111</td>
</tr>
<tr>
<td>commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>client-identity-group</td>
<td>Creates a new client identity group and enters its configuration</td>
<td>page 4-116</td>
</tr>
<tr>
<td>mode group</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.1.29.1 client-identity

Creates a new client identity and enters its configuration mode. Client identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for the identified class of devices in the network. The client-identity feature enables device fingerprinting.

Device fingerprinting is a technique of collecting, analyzing, and identifying traffic patterns originating from remote computing devices. When enabled, device fingerprinting helps to identify a wireless client’s device type. There are two methods of fingerprinting devices: Active and Passive.

Active fingerprinting is based on the fact that traffic patterns vary with varying device types. It involves the sending of requests (HTTP etc.) to devices (clients) and analyzing their response to determine the device type. For example, an invalid request is sent to a device, and its error response is analyzed to identify the device type. Since active device fingerprinting involves sending of packets, the probability of the network getting flooded is very high, especially when many devices are being fingerprinted simultaneously.

Passive fingerprinting involves monitoring of devices to check for known traffic patterns specific to devices based on the protocol, driver implementation etc. This method accurately classifies a client’s TCP/IP configuration, OS fingerprints, wireless settings etc. No packets are sent to the device. Some of the commonly used protocols for passive device fingerprinting are, TCP, DHCP, HTTP etc.

This feature implements DHCP device fingerprinting, which relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

client-identity <CLIENT-IDENTITY-NAME>

Parameters

- client-identity <CLIENT-IDENTITY-NAME>

<table>
<thead>
<tr>
<th>client-identity &lt;CLIENT-IDENTITY-NAME&gt;</th>
<th>Creates a new client identity policy and enters its configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;CLIENT-IDENTITY-NAME&gt; – Specify a client identity policy name. If the client identity policy does not exist, it is created.</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

The following points should be considered when configuring the client identity (device fingerprinting) feature:

1. Ensure that DHCP is enforced on the WLANs. For more information on enforcing DHCP on WLANs, see enforce-dhcp.

2. Successful identification of different device types depends on the uniqueness of the configured fingerprints. DHCP fingerprinting identifies clients based on the patterns (fingerprints) in the DHCP discover and request messages sent by clients. If different operating systems have the same fingerprints, it will be difficult to identify the device type.

3. When associating client identities with a role policy, ensure that the profile/device, under which the role policy is being used, also has an associated client identity group (containing all the client identities used by the role policy).
Examples

rfs4000-229D58(config)#client-identity test
rfs4000-229D58(config-client-identity-test)#?
Client Identity Mode commands:
  dhcp                     Add a DHCP option based match criteria
  dhcp-match-message-type  Specify DHCP message type to match
  no                       Negate a command or set its defaults
  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal
rfs4000-229D58(config-client-identity-test)#
4.1.29.2 client-identity-mode commands

The following table summarizes client identity configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Configures the DHCP option match criteria for device fingerprinting</td>
<td>page 4-112</td>
</tr>
<tr>
<td>dhcp-match-message-type</td>
<td>Configures the DHCP message type for device fingerprinting</td>
<td>page 4-114</td>
</tr>
<tr>
<td>no</td>
<td>Removes the DHCP option (used for client identification) configurations</td>
<td>page 4-115</td>
</tr>
</tbody>
</table>
4.1.29.2.1 dhcp

client-identity-mode commands

Configures the DHCP option match criteria (signature) for the discover and request message types received from wireless clients.

When accessing a network, DHCP discover and request messages are passed between wireless clients and the DHCP server. These messages contain DHCP options and option values that differ from device to device and are based on the DHCP implementation in the device's operating system (OS). Options and option values contained in a client's messages are parsed and compared against the configured DHCP option values to identify the device. Once a device type is identified, the wireless client database is updated with the discovered device type.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp <1-16> message-type [discover|request] [option|option-codes]
dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes] [contains|exact|starts-with] [ascii|hexstring] <WORD>

Parameters

- dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes] [contains|exact|starts-with] [ascii|hexstring] <WORD>

<table>
<thead>
<tr>
<th>dhcp &lt;1-16&gt;</th>
<th>Adds a DHCP option match criteria signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-16&gt;</td>
<td>Specify an index for this DHCP match criteria from 1 - 16.</td>
</tr>
<tr>
<td>Note:</td>
<td>A maximum of 16 match criteria can be configured.</td>
</tr>
</tbody>
</table>

message-type [discover|request] Specifies the message type to which this DHCP match criteria is applicable.

- discover – Applies this match criteria to DHCP discover messages only. Indicates that the fingerprint is only checked with any DHCP discover messages received from any device.
- request – Applies this match criteria to DHCP request messages only. Indicates that the fingerprint is only checked with any DHCP request messages received from any device.

Note: It is recommended to configure client-identity with request messages, because clients rarely send discover messages.

- If the message type is not specified, the fingerprint is checked with all message types (DHCP request and DHCP discover).

option <1-254> The following keywords are common to the 'discover' and 'request' message types:

- option – Configures a DHCP option value, which is used as the match criteria
- <1-254> – Configures a code for this DHCP option from 1 - 254 (except option 53)

option-codes The following keyword is common to the 'discover' and 'request' message types:

- option-codes – Matches criteria based on the DHCP option codes contained in the client's discover/request messages

Note: Devices pass options in their DHCP discover/request messages as option codes, option types, and option value sets. These option codes are extracted and matched against the configured DHCP option codes and a fingerprint is derived. This derived fingerprint is used to identify the device.
Usage Guidelines

The following DHCP options are useful for identifying different device types:

1. Option 55: Used by a DHCP client to request values for specific configuration parameters. It is a list of DHCP option codes and can be in the client's order of preference.

2. Client configured list of DHCP options (all options parsed into a hex string).

3. Option 60: Vendor class identifier. Used to identify the vendor and functionality of a DHCP client (some devices do not set the value of this field).

Though it is possible to use any option to configure a device fingerprint, the use of a combination of one or more of the preceding options to define a device is recommended.

Examples

```
rfs4000-229D58(config-client-identity-test)#dhcp 1 message-type request option 60 exact ascii MSFT\5.0
rfs4000-229D58(config-client-identity-test)#dhcp 2 message-type discover option 2 exact hexstring 012456c22c44

rfs4000-229D58(config-client-identity-test)#show context client-identity test
dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
dhcp 1 message-type request option 60 exact ascii MSFT\5.0
rfs4000-229D58(config-client-identity-test)#
```

Related Commands

```
no
```

Removes a DHCP option signature (match criteria)
4.1.29.2.2 dhcp-match-message-type

`client-identity-mode commands`

Configures the DHCP message type to match

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-match-message-type [all|any|discover|request]

Parameters
- dhcp-match-message-type [all|any|discover|request]

| dhcp-match-message-type [all|any|discover|request] | Specifies the DHCP message type to consider for matching |
|-----------------------------------------------------|--------------------------------------------------------|
| `all` — Matches all message types: discover and request. Indicates that the fingerprint is checked with both the DHCP request and the DHCP discover message. |
| `any` — Matches any message type: discover or request. Indicates that the fingerprint is checked with either the DHCP request or the DHCP discover message. |
| `discover` — Matches discover messages only. Client matches the client identity only if the discover message sent by the client matches. Values configured for request messages are ignored. |
| `request` — Matches request messages only. Client matches the client identity only if the request message sent by the client matches. Values configured for discover messages are ignored. |

Examples

rfs4000-229D58(config-client-identity-test)#dhcp-match-message-type all

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
dhcp 1 message-type request option 60 exact ascii MSFT5.0
dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#

Related Commands

| `no` | Removes the DHCP message type to match |
4.1.29.2.3 no

client-identity-mode commands

Removes the DHCP options match criteria configurations

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [dhcp <1-16>|dhcp-match-message-type]

Parameters

- no [dhcp <1-16>|dhcp-match-message-type]

| dhcp <1-16> | Removes the DHCP option match criteria rule identified by the <1-16> keyword |
| dhcp-match-message-type | Removes the DHCP message type to match |

Examples

The following example shows the client identity ‘test’ settings before the ‘no’ commands are executed:

rfs4000-229D58(config-client-identity-test)#show context
client-identity test
dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
dhcp 1 message-type request option 60 exact ascii MSFT5.0
dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#

The following example shows the client identity ‘test’ settings after the ‘no’ commands are executed:

rfs4000-229D58(config-client-identity-test)#no dhcp 2
rfs4000-229D58(config-client-identity-test)#no dhcp-match-message-type
rfs4000-229D58(config-client-identity-test)#show context
client-identity test
dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#

Related Commands

| dhcp | Configures the DHCP option match criteria for device fingerprinting |
| dhcp-match-message-type | Configures the DHCP message type for device fingerprinting |
4.1.30 client-identity-group

The following table summarizes commands available to enter the client identity group configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identity-group</td>
<td>Creates a new client identity group and enters its configuration mode</td>
<td>page 4-117</td>
</tr>
<tr>
<td>client-identity-group-mode</td>
<td>Invokes the client identity group configuration mode commands</td>
<td>page 4-118</td>
</tr>
<tr>
<td>client-identity</td>
<td>Creates new client identity policy and enters its configuration mode</td>
<td>page 4-108</td>
</tr>
</tbody>
</table>
4.1.30.1 client-identity-group

Conffigures a new client identity group

A client identity group is a collection of client identities. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device Fingerprinting relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

A client identity group can be attached to a profile or device, enabling device fingerprinting on them.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

client-identity-group <CLIENT-IDENTITY-GROUP-NAME>

Parameters

- client-identity-group <CLIENT-IDENTITY-GROUP-NAME>

Examples

rfs4000-229D58(config)#client-identity-group test
rfs4000-229D58(config-client-identity-group-test)#

Client Identity group Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identity</td>
<td>Client identity (DHCP Device Fingerprinting)</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

rfs4000-229D58(config-client-identity-group-test)#
4.1.30.2 client-identity-group-mode commands

The following table summarizes client identity group configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identity</td>
<td>Associates an existing and configured client identity (device fingerprint) with this client identity group</td>
<td>page 4-119</td>
</tr>
<tr>
<td>no</td>
<td>Removes the client identity associated with this client identity group</td>
<td>page 4-115</td>
</tr>
</tbody>
</table>
4.1.30.2.1 client-identity

client-identity-group-mode commands

Associates an existing and configured client identity (device fingerprint) with this client identity group

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>

Parameters

- client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>

| client-identity <CLIENT-IDENTITY-NAME> | Associates a client identity with this group
| precedence <1-10000> | Determines the order in which client identity is used.

Note: The client identity rule is applied based on its precedence value. Lower the value, higher is the precedence. Therefore, a client identity with precedence 5 gets precedence over a client identity having precedence 20.

Examples

The following example shows two client identities created and configured:

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.8.1.0-021D
!
! version 2.1
!
! client-identity TestClientIdentity
dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity test
dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
dhcp 1 message-type request option 60 exact ascii MSFT5.0
dhcp-match-message-type all
! client-identity-group ClientIdentityGroup
client-identity TestClientIdentity precedence 1
!
client-identity-group test
! ip access-list BROADCAST-MULTICAST-CONTROL
   permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
   --More--
rfs4000-229D58(config)#
```
The following example associates client identity ‘test’ with the client identity group ‘test’:

```
rfs4000-229D58(config-client-identity-group-test)#client-identity test precedence 1
```

The following example shows the client identity group ‘test’ with two associated client identities having precedence 1 and 2:

```
rfs4000-229D58(config-client-identity-group-test)#client-identity TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
  client-identity test precedence 1
  client-identity TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#
```

The following example shows the possible client identities:

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.8.1.0-021D
!
! version 2.3
!
 client-identity Android-2-2
   dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
   dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
 client-identity Android-2-3
   dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
   dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
   dhcp 1 message-type request option-codes exact hexstring 353d32393c0c37
   dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
   dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
!
 client-identity Android-2-3-x
   dhcp 10 message-type request option 55 exact hexstring 01792103060f1c333a3b77
   dhcp 11 message-type request option 55 exact hexstring 01792103060f1c2c333a3b77
   dhcp 12 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
 client-identity Android-2-3-3
   dhcp 4 message-type request option 55 exact hexstring 012103061c333a3b
   dhcp 5 message-type request option 60 starts-with ascii dhcpcd-5.2.10
   dhcp 6 message-type request option-codes exact hexstring 3532393c0c37
   dhcp 7 message-type request option-codes exact hexstring 35393c0c37
   dhcp 8 message-type request option-codes exact hexstring 353236393c0c37
!
 client-identity Android-2-3-4
   dhcp 8 message-type request option 55 exact hexstring 012103060f1c333a3b
   dhcp 9 message-type request option 60 starts-with ascii dhcpcd-5.2.10
   dhcp 10 message-type request option 60 starts-with ascii dhcpcd-5.2.10:Linux-3
!
 client-identity Android-2-3-5
   dhcp 8 message-type request option 55 exact hexstring 012103060f1c333a3b
   dhcp 9 message-type request option 60 starts-with ascii dhcpcd-5.2.10:Linux-2.6.36.3:armv7l;p3
```
dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
dhcp 11 message-type request option-codes exact hexstring 353d32393c0c37

client-identity Mac-OS-X

dhcp 3 message-type request option 55 exact hexstring 0103060f775ffcc2c2e2f

client-identity Ubuntu-11

dhcp 2 message-type request option 55 exact hexstring 01lc02030f06770c2c2f1a792a79f9fc2a
dhcp 1 message-type request option-codes exact hexstring 3536120c37
dhcp 3 message-type request option-codes exact hexstring 350c37
dhcp 5 message-type request option-codes exact hexstring 35320c37

client-identity Windows-7

dhcp 2 message-type request option 55 exact hexstring 010f03062c2e21f2f179f92b
dhcp 9 message-type request option 60 exact ascii "MSFT 5.0"

client-identity Windows-8

dhcp 1 message-type request option 55 exact hexstring 010f03062c2e21f2f179f92b
dhcp 5 message-type request option 60 exact ascii "MSFT 5.0"

client-identity Windows-Phone-7-5

dhcp 11 message-type request option 55 exact hexstring 0103060f2c2e2f
dhcp 12 message-type request option-codes exact hexstring 3536323d37

client-identity Windows-XP

dhcp 4 message-type request option 55 exact hexstring 010f03062c2e2f1f21f2b
dhcp 5 message-type request option 60 exact ascii "MSFT 5.0"

client-identity iPhone-iPad

dhcp 10 message-type request option 55 exact hexstring 0103060f77fc
dhcp 1 message-type request option-codes exact hexstring 3537393d32330c
dhcp 2 message-type request option-codes exact hexstring 3537393d32360c
dhcp 3 message-type request option-codes exact hexstring 3537393d3233

client-identity-group default

client-identity Windows-XP precedence 100
client-identity Windows-7 precedence 200
client-identity Android-2-3 precedence 300
client-identity Android-2-2 precedence 400
client-identity Android-2-3-x precedence 500
client-identity Galaxy-Tab precedence 600
client-identity Android-3 precedence 800
client-identity Galaxy-Note precedence 900
client-identity Android-4 precedence 1000
client-identity iPhone-iPad precedence 1100
client-identity Ubuntu-11 precedence 1200
client-identity Windows-Phone-7-5 precedence 1300
client-identity Windows-8 precedence 1500
client-identity Mac-OS-X precedence 1600
client-identity Android-4-1-X precedence 1700
client-identity Android-4-2-X precedence 1800

Related Commands

no

Removes the client identity associated with the client identity group
4.1.30.2.2 no

client-identity-group-mode commands

Removes the client identity associated with the client identity group

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no client-identity <CLIENT-IDENTITY-NAME>

Parameters

- no client-identity <CLIENT-IDENTITY-NAME>

<table>
<thead>
<tr>
<th>no client-identity &lt;CLIENT-IDENTITY-NAME&gt;</th>
<th>Disassociates a specified client identity from this client identity group</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CLIENT-IDENTITY-NAME&gt;</td>
<td>• &lt;CLIENT-IDENTITY-NAME&gt; – Specify the client identity name.</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
rfs4000-229D58(config-client-identity-group-test)#

rfs4000-229D58(config-client-identity-group-test)#no client-identity test
rfs4000-229D58(config)#

Related Commands

<table>
<thead>
<tr>
<th>client-identity</th>
<th>Associates an existing and configured client identity (device fingerprinting) with this client identity group</th>
</tr>
</thead>
</table>
4.1.31 clone

Global Configuration Commands

Creates a replica of an existing object or device. The configuration of the new object or device is an exact copy of the existing object or device configuration. Use this command to copy existing configurations and then modifying only the required parameters.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

clone [TLO|device]

clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>

clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>

Parameters

- clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>

<table>
<thead>
<tr>
<th>TLO &lt;EXISTING-OBJECT-NAME&gt; &lt;NEW-OBJECT-NAME&gt;</th>
<th>Creates a new TLO by cloning an existing top-level object. The new object has the same configuration as the cloned object.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;EXISTING-OBJECT-NAME&gt; – Specify the existing object’s (to be cloned) name</td>
</tr>
<tr>
<td></td>
<td>• &lt;NEW-OBJECT-NAME&gt; – Provide the new object’s name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enter <code>clone</code> and press Tab to list objects available for cloning.</td>
</tr>
</tbody>
</table>

- clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>

<table>
<thead>
<tr>
<th>device &lt;EXISTING-DEVICE-MAC/NAME&gt; &lt;NEW-DEVICE-MAC&gt;</th>
<th>Configures a new device based on an existing device configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;EXISTING-DEVICE-MAC/NAME&gt; – Specify the existing device’s name or MAC address (the device to be cloned)</td>
</tr>
<tr>
<td></td>
<td>• &lt;NEW-DEVICE-MAC&gt; – Provide the new device’s MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enter <code>clone &gt; device</code> and press Tab to list devices available for cloning.</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809(config)#clone rf_domain TechPubs Cloned_TechPubs2
nx9500-6C8809(config)#show context
! Configuration of NX9500 version 5.8.1.0-028D
!
version 2.3
!

rf-domain TechPubs
  location SanJose
  timezone America/Los_Angeles
  country-code us
!
rf-domain Cloned_TechPubs2
  location SanJose
  --More--
nx9500-6C8809(config)#
```
4.1.32 crypto-cmp-policy

Global Configuration Commands

Creates a crypto Certificate Management Protocol (CMP) policy and enters its configuration mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>

Parameters

- crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>

Examples

nx9500-6C8809(config)#crypto-cmp-policy CMP
nx9500-6C8809(config-cmp-policy-CMP)#?

CMP Policy Mode commands:

- ca-server: CMP CA Server configuration commands
- cert-key-size: Set key size for certificate request
- cert-renewal-timeout: Trigger a cert renewal request on timeout
- cross-cert-validate: Validate cross-cert using factory-cert
- no: Negate a command or set its defaults
- subjectAltName: Configure subjectAltName value
- trustpoint: Trustpoint for CMP
- use: Set setting to use

clrscr: Clears the display screen
commit: Commit all changes made in this session
do: Run commands from Exec mode
end: End current mode and change to EXEC mode
exit: End current mode and down to previous mode
help: Description of the interactive help system
revert: Revert changes
service: Service Commands
show: Show running system information
write: Write running configuration to memory or terminal

nx9500-6C8809(config-cmp-policy-CMP)#

Related Commands

| no | Resets values or disables commands |

NOTE: For more information on the crypto CMP policy, see Chapter 29, CRYPTO-CMP-POLICY.
4.1.33 **customize**

- **Global Configuration Command**

Customizes the output of the summary CLI commands. Use this command to define the data displayed as a result of various show commands.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
customize [cdp-lldp-info-column-width|hostname-column-width|show-adoption-status|
show-wireless-meshpoint|show-wireless-meshpoint-accelerated-multicast|
show-wireless-meshpoint-neighbor-stats|show-wireless-meshpoint-neighbor-stats-rf|
show-wireless-mint-client|show-wireless-mint-client-stats|
show-wireless-mint-client-stats-rf|show-wireless-mint-portal|
customize [cdp-lldp-info-column-width|hostname-column-width] <1-64>
customize show-adoption-status (adopted-by, ap-name <1-64>, cdp-lldp-info, config-status, last-adoption, msgs, uptime, version)
customize show-wireless-client (ap-name <1-64>, auth, client-identity <1-32>, bss, enc, hostname <1-64>, ip, last-active, location <1-64>, mac, radio-alias <3-67>, radio-id, radio-type, role <1-32>, state, username <1-64>, vendor, vlan, wlan)
customize show-wireless-client-stats (hostname <1-64>, mac, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)
customize show-wireless-client-stats-rf (average-retry-number, error-rate, hostname <1-64>, mac, noise, q-index, rx-rate, signal, snr, tx-rate)
customize show-wireless-meshpoint-accelerated-multicast (ap-hostname, group-addr, mesh-name, neighbor-hostname, neighbor-ifid, radio-alias, radio-id, radio-mac, subscriptions)
customize show-wireless-meshpoint (ap-mac, cfg-as-root, hops, hostname <1-64>, interface-ids, is-root, mesh-name <1-64>, mpid, next-hop-hostname <1-64>, next-hop-ifid, next-hop-use-time, path-metric, root-bound-time, root-hostname <1-64>, root-mpid)
customize show-wireless-meshpoint-neighbor-stats (ap-hostname <1-64>, neighbor-hostname <1-64>, neighbor-ifid, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)
customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>, average-retry-number, error-rate, neighbor-hostname <1-64>, neighbor-ifid, noise, q-index, rx-rate, signal, snr, t-index, tx-rate)
customize show-wireless-mint-client (client-alias <1-64>, client-bss, portal-alias <1-64>, portal-bss, up-time)
customize show-wireless-mint-client-stats (client-alias <1-64>, portal-alias <1-64>, portal-bss, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)
customize show-wireless-mint-client-stats-rf (average-retry-number, client-alias <1-64>, error-rate, noise, portal-alias <1-64>, portal-bss, q-index, rx-rate, signal, snr, tx-rate)
```
customize show-wireless-mint-portal (client-alias <1-64>, client-bss, portal-alias <1-64>, portal-bss, up-time)

customize show-wireless-mint-portal-stats (client-alias <1-64>, client-bss, portal-alias <1-64>, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)

customize show-wireless-mint-portal-stats-rf (average-retry-number, client-alias <1-64>, client-bss, error-rate, noise, portal-alias <1-64>, q-index, rx-rate, signal, snr, tx-rate)

customize show-wireless-radio (adopt-to, ap-name <1-64>, channel, location <1-64>, num-clients, power, radio-alias <3-67>, radio-id, radio-mac, rf-mode, state)

customize show-wireless-radio-stats (radio-alias <3-67>, radio-id, radio-mac, rx-bytes, tx-bytes, tx-dropped, tx-packets, tx-throughput)

customize show-wireless-radio-stats-rf (average-retry-number, error-rate, noise, q-index, radio-alias <3-67>, radio-id, radio-mac, rx-rate, signal, snr, t-index, tx-rate)

Parameters
• customize [cdp-lldp-info-column-width|hostname-column-width] <1-64>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname-column-width &lt;1-64&gt;</td>
<td>Configures default width of the hostname column in all show command outputs</td>
</tr>
<tr>
<td>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</td>
<td></td>
</tr>
<tr>
<td>cdp-lldp-info-column-width &lt;1-64&gt;</td>
<td>Configures the column width in the show &gt; cdp/lldp &gt; [neighbor</td>
</tr>
<tr>
<td>• &lt;1-64&gt; – Sets the column width from 1 - 64 characters</td>
<td></td>
</tr>
<tr>
<td>• customize show-adoption-status (adopted-by, ap-name &lt;1-64&gt;, cdp-lldp-info, config-status, last-adoption, msgs, uptime, version)</td>
<td>Configures the information displayed in the show &gt; adoption &gt; status command output. Select the columns (information) displayed from the following options: adopted-by, ap-name, cdp-lldp-info, config-status, last-adoption, msgs, uptime, and version. These are recursive parameters and you can select multiple options at a time.</td>
</tr>
<tr>
<td>• Note: The columns displayed by default are: Device-Name, Version, Config-Status, MSGS, Adopted-By, Last-Adoption, and Uptime.</td>
<td></td>
</tr>
<tr>
<td>• Note: Where ever available, you can optionally use the &lt;1-64&gt; parameter to set the column width.</td>
<td></td>
</tr>
<tr>
<td>show-wireless-client (ap-name &lt;1-64&gt;, auth, client-identity &lt;1-32&gt;, bss, enc, hostname &lt;1-64&gt;, ip, last-active, location &lt;1-64&gt;, mac, radio-alias &lt;3-67&gt;, radio-id, radio-type, role &lt;1-32&gt;, state, username &lt;1-64&gt;, vendor, vlan, wlan)</td>
<td>Customizes the show &gt; wireless &gt; client command output</td>
</tr>
<tr>
<td>• Note: The columns displayed by default are: MAC, IPv4, Vendor, Radio-ID, WLAN, VLAN, and State.</td>
<td></td>
</tr>
<tr>
<td>ap-name &lt;1-64&gt;</td>
<td>Includes the ap-name column, which displays the name of the AP with which this client associates</td>
</tr>
<tr>
<td>• &lt;1-64&gt; – Sets the ap-name column width from 1 - 64 characters</td>
<td></td>
</tr>
<tr>
<td>auth</td>
<td>Includes the auth column, which displays the authorization protocol used by the wireless client</td>
</tr>
<tr>
<td>client-identity &lt;1-32&gt;</td>
<td>Includes the client-identity (device type) column, which displays details gathered from DHCP device fingerprinting feature (when enabled). For more information, see client-identity.</td>
</tr>
<tr>
<td>• &lt;1-32&gt; – Sets the client-identity column width from 1 - 32 characters</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bss</td>
<td>Includes the BSS column, which displays the BSS ID the wireless client is associated with</td>
</tr>
<tr>
<td>enc</td>
<td>Includes the enc column, which displays the encryption suite used by the wireless client</td>
</tr>
<tr>
<td>hostname &lt;1-64&gt;</td>
<td>Includes the hostname column, which displays the wireless client's hostname</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</td>
</tr>
<tr>
<td>ip</td>
<td>Includes the IP column, which displays the wireless client's current IP address</td>
</tr>
<tr>
<td>last-active</td>
<td>Includes the last-active column, which displays the time of last activity seen from the wireless client</td>
</tr>
<tr>
<td>location &lt;1-64&gt;</td>
<td>Includes the location column, which displays the location of the client's associated access points</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Sets the location column width from 1 - 64 characters</td>
</tr>
<tr>
<td>mac</td>
<td>Includes the MAC column, which displays the wireless client's MAC address</td>
</tr>
<tr>
<td>radio-alias &lt;3-67&gt;</td>
<td>Includes the radio-alias column, which displays the radio alias with the AP’s hostname and radio interface number in the “HOSTNAME:RX” format</td>
</tr>
<tr>
<td></td>
<td>• &lt;3-64&gt; – Sets the radio-alias column width from 3 - 67 characters</td>
</tr>
<tr>
<td>radio-id</td>
<td>Includes the radio-id column, which displays the radio ID with the AP’s MAC address and radio interface number in the “AA-BB-CC-DD-EE-FF:RX” format</td>
</tr>
<tr>
<td>radio-type</td>
<td>Includes the radio-type column, which displays the wireless client's radio type</td>
</tr>
<tr>
<td>role &lt;1-32&gt;</td>
<td>Includes the role column, which displays the client’s role</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-32&gt; – Sets the role column width from 1 - 32 characters</td>
</tr>
<tr>
<td>state</td>
<td>Includes the state column, which displays the wireless client's current availability state</td>
</tr>
<tr>
<td>username &lt;1-64&gt;</td>
<td>Includes the username column, which displays the wireless client's username</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Specify the username column width from 1 - 64 characters</td>
</tr>
<tr>
<td>vendor</td>
<td>Includes the vendor column, which displays the wireless client's vendor ID</td>
</tr>
<tr>
<td>vlan</td>
<td>Includes the VLAN column, which displays the wireless client's assigned VLAN</td>
</tr>
<tr>
<td>wlan</td>
<td>Includes the WLAN column, which displays the wireless client's assigned WLAN</td>
</tr>
</tbody>
</table>

- customize show-wireless-client-stats (hostname <1-64>, mac, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)

- show-wireless-client-stats
  Customizes the `show > wireless > client > statistics` command output
  **Note:** The columns displayed by default are: MAC, Tx bytes, RX bytes, Tx pkts, Rx pkts, and Tx bps, RX bps, T-Index, and Dropped pkts.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname &lt;1-64&gt;</td>
<td>Includes the hostname column, which displays the wireless client's hostname</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</td>
</tr>
<tr>
<td>mac</td>
<td>Includes the MAC column, which displays the wireless client's MAC address</td>
</tr>
<tr>
<td>rx-bytes</td>
<td>Includes the rx-bytes column, which displays the total number of bytes received by the wireless client</td>
</tr>
<tr>
<td>rx-errors</td>
<td>Includes the rx-error column, which displays the total number of errors received by the wireless client</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rx-packets</td>
<td>Includes the rx-packets column, which displays the total number of packets received by the wireless client</td>
</tr>
<tr>
<td>rx-throughput</td>
<td>Includes the rx-throughput column, which displays the receive throughput at the wireless client</td>
</tr>
<tr>
<td>t-index</td>
<td>Includes the t-index column, which displays the traffic utilization index at the particular wireless client</td>
</tr>
<tr>
<td>tx-bytes</td>
<td>Includes the tx-bytes column, which displays the total number of bytes transmitted by the wireless client</td>
</tr>
<tr>
<td>tx-dropped</td>
<td>Includes the tx-dropped column, which displays the total number of dropped packets by the wireless client</td>
</tr>
<tr>
<td>tx-packets</td>
<td>Includes the tx-packets column, which displays the total number of packets transmitted by the wireless client</td>
</tr>
<tr>
<td>tx-throughput</td>
<td>Includes the tx-throughput column, which displays the transmission throughput at the wireless client</td>
</tr>
</tbody>
</table>

- customize show-wireless-client-stats-rf (average-retry-number, error-rate, host-name <1-64>, mac, noise, q-index, rx-rate, signal, snr, tx-rate)

- **rx-packets**: Includes the rx-packets column, which displays the total number of packets received by the wireless client.
- **rx-throughput**: Includes the rx-throughput column, which displays the receive throughput at the wireless client.
- **t-index**: Includes the t-index column, which displays the traffic utilization index at the particular wireless client.
- **tx-bytes**: Includes the tx-bytes column, which displays the total number of bytes transmitted by the wireless client.
- **tx-dropped**: Includes the tx-dropped column, which displays the total number of dropped packets by the wireless client.
- **tx-packets**: Includes the tx-packets column, which displays the total number of packets transmitted by the wireless client.
- **tx-throughput**: Includes the tx-throughput column, which displays the transmission throughput at the wireless client.

**Note:** The columns displayed by default are: MAC, Signal (dBm), Noise (dBm), SNR (dB), TX Rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%).

- **average-retry-number**: Includes the average-retry-number column, which displays the average number of retransmissions made per packet.
- **error-rate**: Includes the error-rate column, which displays the rate of error for the wireless client.
- **hostname <1-64>**: Includes the hostname column, which displays the wireless client’s hostname.  
  - `<1-64>` – Sets the hostname column width from 1 - 64 characters.
- **mac**: Includes the MAC column, which displays the wireless client’s MAC address.
- **noise**: Includes the noise column, which displays the noise (in dBm) as detected by the wireless client.
- **q-index**: Includes the q-index column, which displays the RF quality index.  
  - **Note:** Higher values indicate better RF quality.
- **rx-rate**: Includes the rx-rate column, which displays the receive rate at the particular wireless client.
- **signal**: Includes the signal column, which displays the signal strength (in dBm) at the particular wireless client.
- **snr**: Includes the snr column, which displays the signal to noise (SNR) ratio (in dB) at the particular wireless client.
- **tx-rate**: Includes the tx-rate column, which displays the packet transmission rate at the particular wireless client.
- customize show-wireless-meshpoint-accelerated-multicast (ap-hostname, group-addr, mesh-name, neighbor-hostname, neighbor-ifid, radio-alias, radio-id, radio-mac, subscriptions)

| show-wireless-meshpoint-accelerated-multicast | Configures the information displayed in the show > wireless > meshpoint > accelerated multicast command output. Select the columns (information) displayed from the following options: ap-hostname, group-addr, mesh-name, neighbor-hostname, neighbor-ifid, radio-alias, radio-id, radio-mac, subscriptions. These are recursive parameters and you can select multiple options at a time.  
**Note:** The columns displayed by default are: Mesh, Radio, Neighbor-IFID, Neighbor-Hostname, Group-MAC, and Subscriptions. |

- customize show-wireless-meshpoint (ap-mac, cfg-as-root, hops, hostname <1-64>, interface-ids, is-root, mesh-name <1-64>, mpid, next-hop-hostname <1-64>, next-hop-ifid, next-hop-use-time, path-metric, root-bound-time, root-hostname <1-64>, root-mpid)

| show-wireless-meshpoint | Customizes the show > wireless > meshpoint command output  
**Note:** The columns displayed by default are: Mesh, Hostname, Hops, Is-Root, Config-As-Root, Root-Hostname, Root-Bound-Time, Path-Metric, Next-Hop-Hostname, and Next-Hop-Use-Time. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-mac</td>
<td>Includes the ap-mac column, which displays the AP's MAC address in the AA-BB-CC-DD-EE-FF format. Applicable only in case of non-controller meshpoints</td>
</tr>
<tr>
<td>cfg-as-root</td>
<td>Includes the cfg-as-root column, which displays the configured root state of the meshpoint</td>
</tr>
<tr>
<td>hops</td>
<td>Includes the hops column, which displays the number of hops to the root for this meshpoint</td>
</tr>
</tbody>
</table>
| hostname <1-64>         | Includes the hostname column, which displays the AP's hostname. Applicable only in case of non-wireless controller meshpoints  
• <1-64> – Sets the hostname column width from 1 - 64 characters |
| interface-ids           | Includes the interface-ids column, which displays the interface identifiers (interfaces used by this meshpoint) |
| is-root                 | Includes the is-root column, which displays the current root state of the meshpoint |
| mesh-name <1-64>        | Includes the mesh-name column, which displays the meshpoint's name  
• <1-64> – Sets the mesh-name column width from 1 - 64 characters |
| mpid                    | Includes the mpid column, which displays the meshpoint identifier in the AA-BB-CC-DD-EE-FF format |
| next-hop-hostname <1-64>| Includes the next-hop-hostname column, which displays the next-hop AP's name (the AP next in the path to the bound root)  
• <1-64> – Sets the next-hop-hostname column width from 1 - 64 characters |
<p>| next-hop-ifid           | Includes the next-hop-ifid column, which displays the next-hop interface identifier in the AA-BB-CC-DD-EE-FF format |
| next-hop-use-time       | Includes the next-hop-use-time column, which displays the time since this meshpoint started using this next hop |
| root-bound-time         | Includes the root-bound-time column, which displays the time since this meshpoint has been bound to the current root |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-hostname &lt;1-64&gt;</td>
<td>Includes the root-hostname column, which displays the root AP’s hostname to which this meshpoint is bound. Set the root-hostname column width from 1 - 64 characters.</td>
</tr>
<tr>
<td>root-mpid</td>
<td>Includes the root-mpid column, which displays the bound root meshpoint identifier in the AA-BB-CC-DD-EE-FF format.</td>
</tr>
</tbody>
</table>

- customize show-wireless-meshpoint-neighbor-stats (ap-hostname <1-64>, neighbor-hostname <1-64>, neighbor-ifid, rx-bytes, rx-errors, rx-packets, tx-bytes, tx-dropped, tx-packets, tx-throughput, t-index)

- customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>, average-retry-number, error-rate, neighbor-hostname <1-64>, neighbor-ifid, noise, q-index, rx-rate, signal, snr, t-rate, tx-rate)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show-wireless-meshpoint-neighbor-stats</td>
<td>Customizes the show &gt; wireless &gt; meshpoint &gt; neighbor &gt; statistics command output. Note: The columns displayed by default are: AP Hostname, Neighbor-IFID, TX bytes, RX bytes, Tx pkts, Rx pkts, Tx (bps), Rx (bps), T-Index (%), and Dropped pkts.</td>
</tr>
<tr>
<td>ap-name &lt;1-64&gt;</td>
<td>Includes the ap-name column, which displays the name of the AP reporting a neighbor. Set the ap-name column width from 1 - 64 characters.</td>
</tr>
<tr>
<td>neighbor-hostname &lt;1-64&gt;</td>
<td>Includes the neighbor-hostname column, which displays the reported neighbor’s hostname. Set the neighbor-hostname column width from 1 - 64 characters.</td>
</tr>
<tr>
<td>neighbor-ifid</td>
<td>Includes the neighbor-ifid column, which displays the neighbor’s interface ID.</td>
</tr>
<tr>
<td>rx-bytes</td>
<td>Includes the rx-bytes column, which displays the total bytes received.</td>
</tr>
<tr>
<td>rx-errors</td>
<td>Includes the rx-error column, which displays the total bytes of error received.</td>
</tr>
<tr>
<td>rx-packets</td>
<td>Includes the rx-packets column, which displays the number of packets received.</td>
</tr>
<tr>
<td>tx-bytes</td>
<td>Includes the tx-bytes column, which displays the total bytes transmitted.</td>
</tr>
<tr>
<td>tx-dropped</td>
<td>Includes the tx-dropped column, which displays the total bytes dropped.</td>
</tr>
<tr>
<td>tx-packets</td>
<td>Includes the tx-packets column, which displays the number of packets transmitted.</td>
</tr>
<tr>
<td>tx-throughput</td>
<td>Includes the tx-throughput column, which displays the neighbor’s transmitted throughput.</td>
</tr>
</tbody>
</table>

- customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>, average-retry-number, error-rate, neighbor-hostname <1-64>, neighbor-ifid, noise, q-index, rx-rate, signal, snr, t-rate, tx-rate)
neighbor-hostname <1-64>
Includes the neighbor-hostname, which displays reported neighbor’s hostname
• <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters

noise
Includes the noise column, which displays the noise level in dBm

q-index
Includes the q-index column, which displays the q-index

rx-rate
Includes the rx-rate column, which displays rate of receiving

signal
Includes the signal column, which displays the signal strength in dBm

snr
Includes the snr column, which displays the signal-to-noise ratio

t-index
Includes the t-index column, which displays t-index

tx-rate
Includes the tx-rate column, which displays rate of transmission

• customize show-wireless-mint-client (client-alias <1-64>, client-bss, portal-alias <1-64>, portal-bss, up-time)

show-wireless-mint-client
Configures the information displayed in the show > wireless > mint > client command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, portal-bss, and up-time. These are recursive parameters and you can select multiple options at a time.

Note: The columns displayed by default are: Portal, Portal-Radio-MAC, Client, Client-Radio-MAC, and Up-Time.

• customize show-wireless-mint-client-stats (client-alias <1-64>, portal-alias <1-64>, portal-bss, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)

show-wireless-mint-client-stats
Configures the information displayed in the show > wireless > mint > client > statistics command output. Select the columns (information) displayed from the following options: client-alias, portal-alias, portal-bss, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput. These are recursive parameters and you can select multiple options at a time.

Note: The columns displayed by default are: Portal, Portal-Radio-MAC, Client, Tx bytes, Rx bytes, TX pkts, Rx pkts, TX (bps), Rx (bps), T-Index (%), and Dropped pkts.

Note: Where ever available, you can optionally use the <1-64> parameter to set the column width.

• customize show-wireless-mint-client-stats-rf (average-retry-number, client-alias <1-64>, error-rate, noise, portal-alias <1-64>, portal-bss, q-index, rx-rate, signal, snr, tx-rate)

show-wireless-mint-client-stats-rf
Configures the information displayed in the show > wireless > mint > client > statistics > rf command output. Select the columns (information) displayed from the following options: average-retry-number, client-alias, error-rate, noise, portal-alias, portal-bss, q-index, rx-rate, signal, snr, and tx-rate. These are recursive parameters and you can select multiple options at a time.

Note: The columns displayed by default are: MAC, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%).

Note: Where ever available, you can optionally use the <1-64> parameter to set the column width.
• **customize show-wireless-mint-portal** *(client-alias <1-64>, client-bss, portal-alias <1-64>, portal-bss, up-time)*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| show-wireless-mint-portal      | Configures the information displayed in the `show > wireless > mint > portal` command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, portal-bss, and up-time. These are recursive parameters and you can select multiple options at a time.  
**Note:** The columns displayed by default are: Client, Client-Radio-MAC, Portal, Portal-Radio-MAC, and Up-Time.  
**Note:** Where ever available, you can optionally use the <1-64> parameter to set the column width. |

• **customize show-wireless-mint-portal-stats** *(client-alias <1-64>, client-bss, portal-alias <1-64>, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| show-wireless-mint-portal-stats | Configures the information displayed in the `show > wireless > mint > portal > statistics` command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput. These are recursive parameters and you can select multiple options at a time.  
**Note:** The columns displayed by default are: Client, Client-Radio-MAC, Portal, Tx bytes, Rx bytes, TX pkts, Rx pkts, TX (bps), Rx (bps), T-Index (%), and Dropped pkts.  
**Note:** Where ever available, you can optionally use the <1-64> parameter to set the column width. |

• **customize show-wireless-mint-portal-stats-rf** *(average-retry-number, client-alias <1-64>, client-bss, error-rate, noise, portal-alias <1-64>, q-index, rx-rate, signal, snr, tx-rate)*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| show-wireless-mint-portal-stats-rf | Configures the information displayed in the `show > wireless > mint > portal > statistics > rf` command output. Select the columns (information) displayed from the following options: average-retry-number, client-alias, client-bss, error-rate, noise, portal-alias, q-index, rx-rate, signal, snr, tx-rate. These are recursive parameters and you can select multiple options at a time.  
**Note:** The columns displayed by default are: Client, Client-Radio-MAC, Portal, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%).  
**Note:** Where ever available, you can optionally use the <1-64> parameter to set the column width. |

• **customize show-wireless-radio** *(adopt-to, ap-name <1-64>, channel, location <1-64>, num-clients, power, radio-alias <3-67>, radio-id, radio-mac, rf-mode, state)*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show-wireless-radio</td>
<td>Customizes the show wireless radio command output</td>
</tr>
<tr>
<td>adopt-to</td>
<td>Includes the adopt-to column, which displays information about the wireless controller adopting this AP</td>
</tr>
</tbody>
</table>
| ap-name <1-64>                  | Includes the ap-name column, which displays information about the AP this radio belongs  
  • <1-64> – Sets the ap-name column width from 1 - 64 characters                                                                                                                                                                           |
| channel                         | Includes the channel column, which displays information about the configured and current channel for this radio                                                                                                                                              |
| **location <1-64>** | Includes the location column, which displays the location of the AP this radio belongs to.  
| | • <1-64> – Sets the location column width from 1 - 64 characters |
| **num-clients** | Includes the num-clients column, which displays the number of clients associated with this radio |
| **power** | Includes the power column, which displays the radio’s configured and current transmit power |
| **radio-alias <3-67>** | Includes the radio-alias column, which displays the radio’s alias (combination of AP’s hostname and radio interface number in the “HOSTNAME:RX” format).  
| | • <3-67> – Sets the radio-alias column width from 3 - 67 characters |
| **radio-id** | Includes the radio-id column, which displays the radio’s ID (combination of AP’s MAC address and radio interface number in the “AA-BB-CC-DD-EE-FF:RX” format) |
| **radio-mac** | Includes the radio-mac column, which displays the radio’s base MAC address |
| **rf-mode** | Includes the rf-mode column, which displays the radio’s operating mode. The radio mode can be 2.4 GHz, 5.0 GHz, or sensor. |
| **state** | Includes the state column, which displays the radio’s current operational state |

- customize show-wireless-radio-stats (radio-alias <3-67>, radio-id, radio-mac, rx-bytes, rx-errors, rx-packets, rx-throughput, tx-bytes, tx-dropped, tx-packets, tx-throughput)
Customize show-wireless-radio-stats-rf (average-retry-number, error-rate, noise, q-index, radio-alias <3-67>, radio-id, radio-mac, rx-rate, signal, snr, t-index, tx-rate)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show-wireless-radio-stats-rf</td>
<td>Customizes the show wireless radio stats RF command output</td>
</tr>
<tr>
<td>average-retry-number</td>
<td>Includes the average-retry-number column, which displays the average number of retransmissions per packet</td>
</tr>
<tr>
<td>error-rate</td>
<td>Includes the error-rate column, which displays the rate of error for the radio</td>
</tr>
<tr>
<td>noise</td>
<td>Includes the noise column, which displays the noise detected by the radio</td>
</tr>
<tr>
<td>q-index</td>
<td>Includes the q-index column, which displays the RF quality index</td>
</tr>
<tr>
<td></td>
<td>Note: Higher values indicate better RF quality.</td>
</tr>
<tr>
<td>radio-alias &lt;3-67&gt;</td>
<td>Includes the radio-alias column, which displays the radio’s alias (combination of AP’s hostname and radio interface number in the “HOSTNAME:RX” format)</td>
</tr>
<tr>
<td></td>
<td>• &lt;3-67&gt; – Sets the radio-alias column width from 3 - 67 characters</td>
</tr>
<tr>
<td>radio-id</td>
<td>Includes the radio-id column, which displays the radio’s ID (combination of AP’s MAC address and radio interface number in the “AA-BB-CC-DD-EE-FF:RX” format)</td>
</tr>
<tr>
<td>radio-mac</td>
<td>Includes the radio-mac column, which displays the radio’s base MAC address</td>
</tr>
<tr>
<td>rx-rate</td>
<td>Includes the rx-rate column, which displays the receive rate at the particular radio</td>
</tr>
<tr>
<td>signal</td>
<td>Includes the signal column, which displays the signal strength at the particular radio</td>
</tr>
<tr>
<td>snr</td>
<td>Includes the snr column, which displays the signal-to-noise ratio at the particular radio</td>
</tr>
<tr>
<td>t-index</td>
<td>Includes the t-index column, which displays the traffic utilization index at the particular radio</td>
</tr>
<tr>
<td>tx-rate</td>
<td>Includes the tx-rate column, which displays the packet transmission rate at the particular radio</td>
</tr>
</tbody>
</table>

Examples

The following example shows the shows the `show > adoption > status` command output before customizing the output:

```
rfs7000-6DCD4B(config)#show adoption status
-------------------------------------------------------------------------
DEVICE-NAME VERSION CFG-STAT MSGS ADOPTED-BY LAST-ADOPTION UPTIME
rfs6000-81742D 5.8.1.0-028D configured No rfs7000-6DCD4B 0 days 05:03:18 0 days 05:06:26
-------------------------------------------------------------------------
Total number of devices displayed: 1
rfs7000-6DCD4B(config)#
```

```
rfs7000-6DCD4B(config)#customize show-adoption-status adopted-by ap-name config-status last-adoption
rfs7000-6DCD4B(config)#commit
```
The following example shows the show > adoption > status command output after customizing the output:

```
rfs7000-6DCD4B(config)#show adoption status
------------------------------------------------------------------------
ADOPTED-BY        DEVICE-NAME       CFG-STAT         LAST-ADOPTION
------------------------------------------------------------------------
rfs7000-6DCD... rfs6000-81742D    *configured        0 days 05:10:01
------------------------------------------------------------------------
```

Total number of devices displayed: 1
```
rfs7000-6DCD4B(config)#
```

Use the no > customize > show-adoption-status command to revert back to the default format.
```
rfs7000-6DCD4B(config)#no customize show-adoption-status
rfs7000-6DCD4B(config)#commit
rfs7000-6DCD4B(config)#
```

```
------------------------------------------------------------------------
DEVICE-NAME    VERSION      CFG-STAT  MSGS  ADOPTED-BY     LAST-ADOPTION     UPTIME
------------------------------------------------------------------------
rfs6000-81742D 5.8.1.0-028D configured No rfs7000-6DCD4B 3 days 22:51:23 3 days 22:54:30
------------------------------------------------------------------------
```

Total number of devices displayed: 1
```
rfs7000-6DCD4B(config)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Restores custom CLI settings to default</td>
</tr>
<tr>
<td>wireless</td>
<td>Displays wireless configuration and other information</td>
</tr>
</tbody>
</table>
### 4.1.34 device

> **Global Configuration Commands**

Enables simultaneous configuration of multiple devices

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
device {containing|filter}
```

```
device {containing <STRING>} {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|t5|vx9000]}
```

**Parameters**

- **device {containing <STRING>} {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600|t5|vx9000]}

<table>
<thead>
<tr>
<th>device</th>
<th>Enters a device’s configuration mode. Use this command to simultaneously configure devices having similar configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>containing &lt;STRING&gt;</td>
<td>Optional. Configures the string to search for in the device’s hostname. All devices having hostnames containing the string specified here are filtered, and can be configured simultaneously.</td>
</tr>
<tr>
<td>&lt;STRING&gt;</td>
<td>- Specify the string to search for in the device’s hostname.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>filter type &lt;DEVICE-TYPE&gt;</th>
<th>Optional. Filters out a specific device type. After specifying the hostname string, select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600, t5, and VX9000 (V-WLC).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: The t5 option is applicable only on the RFS7000, NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, and NX9600 platforms.</td>
<td></td>
</tr>
<tr>
<td>Note: The VX9000 option is applicable only to the NX9000, NX9500, NX9510, and NX9600 platforms.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>device</th>
<th>Configures a basic device profile</th>
</tr>
</thead>
</table>

```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes multiple devices from the network</td>
</tr>
</tbody>
</table>
4.1.35 device-categorization

Global Configuration Commands

Categorizes devices as sanctioned or neighboring. Categorization of devices enables quick identification and blocking of unsanctioned devices in the network.

The following table summarizes the device categorization mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>device-categorization</td>
<td>Creates a device categorization list and enters its configuration mode</td>
<td>page 4-139</td>
</tr>
<tr>
<td>device-categorization-mode</td>
<td>Summarizes device categorization list configuration mode commands</td>
<td>page 4-140</td>
</tr>
</tbody>
</table>
4.1.35.1 device-categorization

- **device-categorization**

  Configures a device categorization list

  Proper classification and categorization of devices (access points, clients etc.) helps suppress unnecessary unauthorized access point alarms, allowing network administrators to focus on alarms on devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization.

  Authorized access points and clients are generally known to you and conform with your organization’s security policies. Unauthorized devices are those detected as interoperating within the network, but are not approved. These devices should be filtered to avoid jeopardizing the data within a managed network. Use this command to apply the neighboring and sanctioned (approved) filters on peer devices operating within a wireless controller or access point’s radio coverage area. Detected client MAC addresses can also be filtered based on their classification.

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

  **Syntax**
  
  device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>

  **Parameters**
  - device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>

  **Examples**
  
  rfs7000-37FABE(config)#device-categorization rfs7000
  rfs7000-37FABE(config-device-categorization-rfs7000)#?

  Device Category Mode commands:
  - mark-device  Add a device
  - no           Negate a command or set its defaults
  - clrscr       Clears the display screen
  - commit       Commit all changes made in this session
  - do           Run commands from Exec mode
  - end          End current mode and change to EXEC mode
  - exit         End current mode and down to previous mode
  - help         Description of the interactive help system
  - revert       Revert changes
  - service      Service Commands
  - show         Show running system information
  - write        Write running configuration to memory or terminal

  rfs7000-37FABE(config-device-categorization-rfs7000)#

  **Related Commands**

  - **no**  Removes an existing device categorization list
4.1.35.2 device-categorization-mode commands

The following table summarizes device categorization configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>mark-device</td>
<td>Adds a device to the device categorization list</td>
<td>page 4-141</td>
</tr>
<tr>
<td>no</td>
<td>Removes a device from the device categorization list</td>
<td>page 4-142</td>
</tr>
</tbody>
</table>
4.1.35.2.1 mark-device

device-categorization-mode commands

Adds a device to the device categorization list as sanctioned or neighboring. Devices are further classified as AP or client.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

mark-device <1-1000> [sanctioned|neighboring] [ap|client]
mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>|ssid <SSID> {mac <MAC>}}
mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}

Parameters

- mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>|ssid <SSID> {mac <MAC>}}

| <1-1000> | Configures the device categorization entry index number |
| sanctioned | Marks a device as sanctioned. A sanctioned device is authorized to use network resources. |
| neighboring | Marks a device as neighboring. A sanctioned device is a neighbor in the same network as this device. |
| ap {mac <MAC>|ssid <SSID>} | Marks a specified AP as sanctioned or neighboring based on its MAC address or SSID |
| • mac <MAC> – Optional. Specify the AP’s MAC address |
| • ssid <SSID> – Optional. Specify the AP’s SSID. After specifying the SSID, you can optionally specify its MAC address. |
| Note: All APs are marked if no specific MAC address or SSID is provided. |

- mark-device [sanctioned|neighboring] client {mac <MAC>}

| <1-1000> | Configures the device categorization entry index number |
| sanctioned | Marks the wireless client as sanctioned. A sanctioned device is authorized to use network resources. |
| neighboring | Marks the wireless client as neighboring. A sanctioned device is a neighbor in the same network as this device. |
| client {mac <MAC>} | Marks a specified wireless client as sanctioned or neighboring based on its MAC address |
| • mac <MAC> – Optional. Specify the wireless client’s MAC address. |

Examples

rfs7000-37FABE(config-device-categorization-rfs7000)#mark-device 1 sanctioned ap mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#show context
device-categorization rfs7000
mark-device 1 sanctioned ap mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#

Related Commands

no | Removes an entry from the device categorization list |
4.1.35.2.2 no

Removes a device from the device categorization list

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
no mark-device <1-1000> [neighboring|sanctioned] [ap|client] {mac <MAC>}
no mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
no mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>|ssid <SSID> {mac <MAC>}}

Parameters
- no <PARAMETERS>

| no <PARAMETERS> | Removes a mark device (AP or wireless client) entry from this device categorization list |

Examples
The following example shows the device categorization list 'rfs7000' settings before the 'no' command is executed:

rfs7000-37FABE(config-device-categorization-rfs7000)#show context device-categorization rfs7000
  mark-device 1 sanctioned ap mac 11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#

rfs7000-37FABE(config-device-categorization-rfs7000)#no mark-device 1 sanctioned ap mac 11-22-33-44-55-66

The following example shows the device categorization list 'rfs7000' settings after the 'no' command is executed:

rfs7000-37FABE(config-device-categorization-rfs7000)#show context device-categorization rfs7000
rfs7000-37FABE(config-device-categorization-rfs7000)#

Related Commands

- mark-device | Adds a device to a list of sanctioned or neighboring devices |
4.1.36 **dhcp-server-policy**

> **Global Configuration Commands**

Configures DHCPv4 server policy parameters, such as class, address range, and options. A new policy is created if it does not exist.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dhcp-server-policy <DHCP-SERVER-POLICY-NAME>

**Parameters**

- dhcp-server-policy <DHCP-SERVER-POLICY-NAME>

| <DHCP-SERVER-POLICY-NAME> | Specify the DHCPv4 server policy name. If the policy does not exist, it is created. |

**Examples**

rfs7000-37FABE(config)#dhcp-server-policy test
rfs7000-37FABE(config-dhcp-policy-test)#?

DHCP policy Mode commands:

- bootp: BOOTP specific configuration
- dhcp-class: Configure DHCP class (for address allocation using DHCP user-class options)
- dhcp-pool: Configure DHCP server address pool
- dhcp-server: Activating dhcp server based on criteria
- no: Negate a command or set its defaults
- option: Define DHCP server option
- ping: Specify ping parameters used by DHCP Server
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test)#

**Related Commands**

- **no** Removes an existing DHCP server policy

---

**NOTE:** For more information on DHCP policy, see *Chapter 12, DHCP-SERVER-POLICY.*
4.1.37 dhcpv6-server-policy

Global Configuration Commands

Creates a DHCPv6 server policy and enters its configuration mode.

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non-duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

When configured and applied to a device, the DHCPv6 server policy enables the device to function as a stateless DHCPv6 server.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcpv6-server-policy <DHCPv6-SERVER-POLICY-NAME>

Parameters

- dhcpv6-server-policy <DHCPv6-SERVER-POLICY-NAME>

Examples

rfs7000-6DCD4B(config)#dhcpv6-server-policy test
rfs7000-6DCD4B(config-dhcpv6-server-policy-test)#?

DHCPv6 server policy Mode commands:

dhcpv6-pool Configure DHCPv6 server address pool
no Negate a command or set its defaults
option Define DHCPv6 server option
restrict-vendor-options Restrict vendor specific options to be sent in server reply
server-preference Server preference value sent in the reply, by the server to client
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
show Show running configuration information
write Write running configuration to memory or terminal

rfs7000-6DCD4B(config-dhcpv6-server-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an existing DHCPv6 server policy</td>
</tr>
</tbody>
</table>
NOTE: For more information on DHCP policy, see Chapter 12, DHCP-SERVER-POLICY.
4.1.38  **dns-whitelist**

- **Global Configuration Commands**
  
  Configures a DNS whitelist. A DNS whitelist is a list of domains allowed access to the network.
  
The following table lists DNS Whitelist configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dns-whitelist</code></td>
<td>Creates a DNS whitelist and enters its configuration mode</td>
<td>page 4-147</td>
</tr>
<tr>
<td><code>dns-whitelist-mode</code></td>
<td>Summarizes DNS whitelist configuration mode commands</td>
<td>page 4-148</td>
</tr>
</tbody>
</table>

*Table 4.14  DNS-Whitelist Config Commands*
4.1.38.1 dns-whitelist

`dns-whitelist` command

Configures a DNS whitelist. A DNS whitelist is a list of allowed DNS destination IP addresses pre-approved to access a controller, service platform, or access point managed captive portal.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dns-whitelist <DNS-WHITELIST-NAME>

Parameters

- `dns-whitelist <DNS-WHITELIST-NAME>`

<table>
<thead>
<tr>
<th>&lt;DNS-WHITELIST-NAME&gt;</th>
<th>Specify the DNS whitelist name. If the whitelist does not exist, it is created.</th>
</tr>
</thead>
</table>

Examples

rfs7000-37FABE(config)#dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#?

DNS Whitelist Mode commands:

- no Negate a command or set its defaults
- permit Match a host
- clrscr Clears the display screen
- commit Commit all changes made in this session
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-dns-whitelist-test)#

Related Commands

- `no` Removes an existing DNS Whitelist
The following table summarizes DNS Whitelist configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>Permits a host, existing on a DNS whitelist, access to the network or captive portal</td>
<td>page 4-149</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts to default</td>
<td>page 4-150</td>
</tr>
</tbody>
</table>
4.1.38.2.1 permit

A whitelist is a list of host names and IP addresses permitted access to the network or captive portal. This command adds a host or destination IP address to the DNS whitelist.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit <IPv4/IPv6/HOSTNAME> {suffix}
```

**Parameters**

- `permit <IPv4/IPv6/HOSTNAME> {suffix}`

<table>
<thead>
<tr>
<th><code>&lt;IPv4/IPv6/HOSTNAME&gt;</code></th>
<th>Adds a device to the DNS whitelist</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--</code></td>
<td>Provide a hostname or numerical IPv4 or IPv6 address for each destination IP address or host included in the whitelist.</td>
</tr>
</tbody>
</table>

**Note:** A maximum of 256 entries can be made.

<table>
<thead>
<tr>
<th>suffix</th>
<th>Optional. Matches any hostname or domain name including the specified name as suffix</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config-dns-whitelist-test)#permit example_company.com suffix

rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
permit example_company.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#
```

**Related Commands**

- `no` Removes a DNS whitelist entry
4.1.38.2.2 **no**

**dns-whitelist-mode commands**

Removes a specified host or IP address from the DNS whitelist, and prevents it from accessing network resources.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no permit <IPv4/IPv6/HOSTNAME>
```

**Parameters**

- `no permit <IPv4/IPv6/HOSTNAME>`

**Examples**

```
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#
```

```
rfs7000-37FABE(config-dns-whitelist-test)#no permit example_company.com
```

```
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#
```

**Related Commands**

- **permit** Adds a device to the DNS whitelist
4.1.39 **end**

*Global Configuration Commands*

Ends and exits the current mode and moves to the PRIV EXEC mode.

The prompt changes to the PRIV EXEC mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
end
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config)#end
rfs7000-37FABE#
```
### 4.1.40 event-system-policy

*Global Configuration Commands*

Configures how events are supported. Each event can be configured individually to perform an action such as sending an e-mail or forwarding a notification.

The following table lists event system configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>event-system-policy</td>
<td>Creates an event system policy and enters its configuration mode</td>
<td>page 4-153</td>
</tr>
<tr>
<td>event-system-policy-mode</td>
<td>Summarizes event system policy configuration mode commands</td>
<td>page 4-154</td>
</tr>
</tbody>
</table>
4.1.40.1 event-system-policy

`event-system-policy`

Configures a system wide events handling policy

Event system policies enable administrators to create notification mechanisms using one, some, or all of the SNMP, syslog, controller forwarding, or email notification options available to the controller or service platform. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication or encryption, and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices.

To view an existing event system policy configuration details, use the `show > event-system-policy` command.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`event-system-policy <EVENT-SYSTEM-POLICY-NAME>`

**Parameters**
- `event-system-policy <EVENT-SYSTEM-POLICY-NAME>`

| `<EVENT-SYSTEM-POLICY-NAME>` | Specify the event system policy name. If the policy does not exist, it is created. |

**Examples**

```plaintext
rfs7000-37FABE(config)#event-system-policy event-testpolicy
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#?
```

Event System Policy Mode commands:
- `event` Configure an event
- `no` Negate a command or set its defaults
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```plaintext
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#
```

**Related Commands**

- `no` Removes an event system policy
4.1.40.2 event-system-policy-mode commands

The following table summarizes event system policy configuration mode commands:

Table 4.17 Event-System-Policy Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
<td>Configures an event</td>
<td>page 4-155</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts to default</td>
<td>page 4-166</td>
</tr>
</tbody>
</table>
4.1.40.2.1 event

*event-system-policy-mode commands*

Configures an event and sets the action performed when the event happens

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog) [default|on|off]

The event types are:

rfs7000-37FABE(config-event-system-policy-testpolicy)#event ?

aaa AAA/Radius module
adopt-service Adoption Service
adv-wips Adv-wips module
ap Access Point module
captive-portal Captive Portal
certmgr Certificate Manager (Not valid for NCAP/MCN)
certmgr-lite Lite version of certificate manager (NCAP & MCN) only
cfgd Cfgd module
cluster Cluster module
crm Critical Resource Monitoring
device Device module
dhcpsvr DHCP Configuration Daemon
diag Diag module
dot11 802.11 management module
dot1x 802.1X Authentication
fwu Firmware update module
isdn Isdn module
l2tpv3 Layer 2 Tunneling Protocol Version 3
licmgr License module
mesh Mesh module
mgmt Management Services
nsm Network Services Module
pm Process-monitor module
radconf Radius ConfigurationDaemon
rasset Roaming-Assist module
radio Radio module
smrt Smart-rf module
smtpnot Smtpnot module
system System module
test Test module
vrrp Virtual Router Redundancy Protocol
wips Wireless IPS module

rfs7000-37FABE(config-event-system-policy-testpolicy)#

---

**NOTE:** The parameter values for <EVENT-TYPE> and <EVENT-NAME> are summarized in the table under the Parameters section.
### Parameters

- **event** `<EVENT-TYPE> <EVENT-NAME>` (email, forward-to-switch, snmp, syslog) [default|on|off]

<table>
<thead>
<tr>
<th><code>&lt;event-type&gt;</code></th>
<th><code>&lt;event-name&gt;</code></th>
</tr>
</thead>
</table>
| aaa            | Enables and configures the logging of authentication, authorization, and accounting related event messages  
|               | • radius-discon-msg – RADIUS disconnection message  
|               | • radius-session-expired – RADIUS session expired message  
|               | • radius-session-not-started – RADIUS session not started message  
|               | • radius-vlan-update – RADIUS VLAN update message  
| adopt-services | Enables and configures the logging of adopted services related events  
| adv-wips       | Enables and configures the logging of advanced WIPS related events  
| ap             | Enables and configures the logging of AP related event messages  
|               | • adopted – Event AP adopted message  
|               | • adopted-to-controller – Event AP adopted to wireless controller message  
|               | • ap-adopted – Event access port adopted message  
|               | • ap-autoup-done – Event AP autoup done message  
|               | • ap-autoup-fail – Event AP autoup fail message  
|               | • ap-autoup-needed – Event AP autoup needed message  
|               | • ap-autoup-no-need – Event AP autoup not needed message  
|               | • ap-autoup-reboot – Event AP autoup reboot message  
|               | • ap-autoup-timeout – Event AP autoup timeout message  
|               | • ap-autoup-ver – Event AP autoup version message  
|               | • ap-reset-detected – Event access port reset detected message  
|               | • ap-reset-request – Event access port user requested reset message  
|               | • ap-timeout – Event access port timed out message  
|               | • ap-unadopted – Event access port unadopted message  
|               | • image-parse-failure – Event image parse failure message  
|               | • legacy-auto-update – Event legacy auto update message  
|               | • no-image-file – Event no image file message  
|               | • offline – Event AP detected as offline  
|               | • online – Event offline AP detected as online  
|               | • reset – Event reset message  
|               | • sw-conn-lost – Event software connection lost message  
|               | • unadopted – Event unadopted message  
| captive-portal | Enables and configures the logging of captive portal (hotspot) related event messages  
|               | • allow-access – Event client allowed access message  
|               | • auth-failed – Event authentication failed message  
|               | • auth-success – Event authentication success message  
|               | • client-disconnect – Event client disconnected message  
|               | • client-removed – Event client removed message  
|               | • data-limit-exceed – Event client data limit exceed message  
|               | • flex-log-access – Event flexible log access granted to client message  
|               | Contd..
<table>
<thead>
<tr>
<th><code>&lt;event-type&gt;</code></th>
<th><code>&lt;event-name&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>inactivity-timeout</td>
<td>Event client time-out due to inactivity message</td>
</tr>
<tr>
<td>page-cre-failed</td>
<td>Event page creation failure message</td>
</tr>
<tr>
<td>purge-client</td>
<td>Event client purged message</td>
</tr>
<tr>
<td>session-timeout</td>
<td>Event session timeout message</td>
</tr>
<tr>
<td>vlan-switch</td>
<td>Event client switched VLAN</td>
</tr>
<tr>
<td>certmgr</td>
<td>Enables and configures the logging of certificate manager related event messages (Not applicable to AP6511 and AP6521)</td>
</tr>
<tr>
<td>ca-cert-actions-failure</td>
<td>Event CA certificate actions failure message</td>
</tr>
<tr>
<td>ca-cert-actions-success</td>
<td>Event CA certificate actions success message</td>
</tr>
<tr>
<td>ca-key-actions-failure</td>
<td>Event CA key actions failure message</td>
</tr>
<tr>
<td>ca-key-actions-success</td>
<td>Event CA key actions success message</td>
</tr>
<tr>
<td>cert-expiry</td>
<td>Event certificate expiry message</td>
</tr>
<tr>
<td>crl-actions-failure</td>
<td>Event Certificate Revocation List (CRL) actions failure message</td>
</tr>
<tr>
<td>crl-actions-success</td>
<td>Event CRL actions success message</td>
</tr>
<tr>
<td>csr-export-failure</td>
<td>Event CSR export failure message</td>
</tr>
<tr>
<td>csr-export-success</td>
<td>Event CSR export success message</td>
</tr>
<tr>
<td>delete-trustpoint-action</td>
<td>Event delete trustpoint action message</td>
</tr>
<tr>
<td>export-trustpoint</td>
<td>Event export trustpoint message</td>
</tr>
<tr>
<td>import-trustpoint</td>
<td>Event import trustpoint message</td>
</tr>
<tr>
<td>rsa-key-actions-failure</td>
<td>Event RSA key actions failure message</td>
</tr>
<tr>
<td>rsa-key-actions-success</td>
<td>Event RSA key actions success message</td>
</tr>
<tr>
<td>svr-cert-actions-success</td>
<td>Event server certificate actions success message</td>
</tr>
<tr>
<td>svr-cert-actions-failure</td>
<td>Event server certificate actions failure message</td>
</tr>
<tr>
<td>certmgr-lite</td>
<td>Enables and configures logging of certificate manager (lite version) related event messages (applicable only to AP621, AP6521 and AP6511)</td>
</tr>
<tr>
<td>cfgd</td>
<td>Enables and configures the logging of configuration daemon module related event messages</td>
</tr>
<tr>
<td>acl-attached-altered</td>
<td>Event Access List (ACL) attached altered message</td>
</tr>
<tr>
<td>acl-rule-altered</td>
<td>Event ACL rule altered message</td>
</tr>
<tr>
<td>cluster</td>
<td>Enables and configures logging of cluster module related event messages</td>
</tr>
<tr>
<td>cmaster-cfg-update-fail</td>
<td>Event cluster master config update failed message</td>
</tr>
<tr>
<td>max-exceeded</td>
<td>Event maximum cluster count exceeded message</td>
</tr>
<tr>
<td>state-change</td>
<td>Event cluster state change (active/inactive)</td>
</tr>
<tr>
<td>state-change-active</td>
<td>Event cluster state change to active</td>
</tr>
<tr>
<td>state-change-inactive</td>
<td>Event cluster state change to inactive</td>
</tr>
<tr>
<td>state-retain-active</td>
<td>Event cluster state retained as active</td>
</tr>
<tr>
<td>crm</td>
<td>Enables and configures the logging of Critical Resource Monitoring (CRM) related event messages</td>
</tr>
<tr>
<td>critical-resource-down</td>
<td>Event Critical Resource Down message</td>
</tr>
<tr>
<td>critical-resource-up</td>
<td>Event Critical Resource Up message</td>
</tr>
<tr>
<td>device</td>
<td>Enables and configures the logging of device module related event messages</td>
</tr>
<tr>
<td><strong>&lt;event-type&gt;</strong></td>
<td><strong>&lt;event-name&gt;</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>dhcpsvr</td>
<td>Enables and configures the logging of DHCP server related event messages</td>
</tr>
<tr>
<td></td>
<td>• dhcp-start – Event DHCP server started message</td>
</tr>
<tr>
<td></td>
<td>• dhcpsvr-stop – Event DHCP server stopped message</td>
</tr>
<tr>
<td></td>
<td>• relay-iface-no-ip – Event no IP address on DHCP relay interface message</td>
</tr>
<tr>
<td></td>
<td>• relay-no-iface – Event no interface for DHCP relay message</td>
</tr>
<tr>
<td></td>
<td>• relay-start – Event relay agent started</td>
</tr>
<tr>
<td></td>
<td>• relay-stop – Event DHCP relay agent stopped</td>
</tr>
<tr>
<td>diag</td>
<td>Enables and configures the logging of diagnostics module related event messages</td>
</tr>
<tr>
<td></td>
<td>• autogen-tech-sprt – Event autogen technical support message</td>
</tr>
<tr>
<td></td>
<td>• buf-usage – Event buffer usage message</td>
</tr>
<tr>
<td></td>
<td>• cpu-load – Event CPU load message</td>
</tr>
<tr>
<td></td>
<td>• cpu-usage-too-high – Event CPU usage high message</td>
</tr>
<tr>
<td></td>
<td>• cpu-usage-too-high-recover – Event recovery from high CPU usage message</td>
</tr>
<tr>
<td></td>
<td>• disk-usage – Event disk usage message</td>
</tr>
<tr>
<td></td>
<td>• elapsed-time – Event elapsed time message</td>
</tr>
<tr>
<td></td>
<td>• fan-underspeed – Event fan underspeed message</td>
</tr>
<tr>
<td></td>
<td>• fd-count – Event forward count message</td>
</tr>
<tr>
<td></td>
<td>• free-flash-disk – Event free flash disk message</td>
</tr>
<tr>
<td></td>
<td>• free-flash-inodes – Event free flash inodes message</td>
</tr>
<tr>
<td></td>
<td>• free-nvram-disk – Event free nvram disk message</td>
</tr>
<tr>
<td></td>
<td>• free-nvram-inodes – Event free nvram inodes message</td>
</tr>
<tr>
<td></td>
<td>• free-ram – Event free ram message</td>
</tr>
<tr>
<td></td>
<td>• free-ram-disk – Event free ram disk message</td>
</tr>
<tr>
<td></td>
<td>• free-ram-inodes – Event free ram inodes message</td>
</tr>
<tr>
<td></td>
<td>• head-cache-usage – Event head cache usage message</td>
</tr>
<tr>
<td></td>
<td>• high-temp – Event high temp message</td>
</tr>
<tr>
<td></td>
<td>• ip-dest-usage – Event ip destination usage message</td>
</tr>
<tr>
<td></td>
<td>• led-identify – Event led identify message</td>
</tr>
<tr>
<td></td>
<td>• low-temp – Event low temp message</td>
</tr>
<tr>
<td></td>
<td>• mem-usage-too-high – Event memory usage high message</td>
</tr>
<tr>
<td></td>
<td>• mem-usage-too-high-recover – Event recovery from high memory usage message</td>
</tr>
<tr>
<td></td>
<td>• new-led-state – Event new led state message</td>
</tr>
<tr>
<td></td>
<td>• over-temp – Event over temp message</td>
</tr>
<tr>
<td></td>
<td>• over-voltage – Event over voltage message</td>
</tr>
<tr>
<td></td>
<td>• poe-init-fail – Event PoE init fail message</td>
</tr>
<tr>
<td></td>
<td>• poe-power-level – Event PoE power level message</td>
</tr>
<tr>
<td></td>
<td>• poe-read-fail – Event PoE read fail message</td>
</tr>
<tr>
<td></td>
<td>• poe-state-change – Event PoE state change message</td>
</tr>
<tr>
<td></td>
<td>• raid-degraded – Event Redundant Array of Independent Disks (RAID) degraded message</td>
</tr>
</tbody>
</table>

Contd..
<table>
<thead>
<tr>
<th>&lt;event-type&gt;</th>
<th>&lt;event-name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>raid-error</td>
<td>Event RAID error message</td>
</tr>
<tr>
<td>ram-usage</td>
<td>Event ram usage message</td>
</tr>
<tr>
<td>under-voltage</td>
<td>Event under voltage message</td>
</tr>
<tr>
<td>wd-reset-sys</td>
<td>Event wd reset system message</td>
</tr>
<tr>
<td>wd-state-change</td>
<td>Event wd state change message</td>
</tr>
<tr>
<td>dot11</td>
<td>Enables and configures the logging of 802.11 management module related event messages</td>
</tr>
<tr>
<td>client-assoc-ignored</td>
<td>Wireless client association ignored event message</td>
</tr>
<tr>
<td>client-associated</td>
<td>Wireless client associated event message</td>
</tr>
<tr>
<td>client-denied-assoc</td>
<td>Event client denied association message</td>
</tr>
<tr>
<td>client-disassociated</td>
<td>Wireless client disassociated message</td>
</tr>
<tr>
<td>country-code</td>
<td>Event country code message</td>
</tr>
<tr>
<td>country-code-error</td>
<td>Event country code error message</td>
</tr>
<tr>
<td>eap-cached-keys</td>
<td>Event Extensible Authentication Protocol (EAP) cached keys message</td>
</tr>
<tr>
<td>eap-client-timeout</td>
<td>Event EAP client timeout message</td>
</tr>
<tr>
<td>eap-failed</td>
<td>Event EAP failed message</td>
</tr>
<tr>
<td>eap-opp-cached-keys</td>
<td>Event EAP opp cached keys message</td>
</tr>
<tr>
<td>eap-preauth-client-timeout</td>
<td>Event EAP pre authentication client timeout message</td>
</tr>
<tr>
<td>eap-preauth-failed</td>
<td>Event EAP pre authentication failed message</td>
</tr>
<tr>
<td>eap-preauth-server-timeout</td>
<td>Event EAP pre authentication server timeout message</td>
</tr>
<tr>
<td>eap-preauth-success</td>
<td>Event EAP pre authentication success message</td>
</tr>
<tr>
<td>eap-server-timeout</td>
<td>Event EAP server timeout message</td>
</tr>
<tr>
<td>eap-success</td>
<td>Event EAP success message</td>
</tr>
<tr>
<td>ft-roam-success</td>
<td>Event client fast BSS transition message</td>
</tr>
<tr>
<td>gal-rx-request</td>
<td>Event GAL request received event message</td>
</tr>
<tr>
<td>gal-tx-response</td>
<td>Event response sent to GAL request message</td>
</tr>
<tr>
<td>gal-validate-failed</td>
<td>Event GAL validation failed message</td>
</tr>
<tr>
<td>gal-validate-req</td>
<td>Event GAL validation request message</td>
</tr>
<tr>
<td>gal-validate-success</td>
<td>Event GAL validation success message</td>
</tr>
<tr>
<td>kerberos-client-success</td>
<td>Event client Kerberos authentication success message</td>
</tr>
<tr>
<td>kerberos-wlan-failed</td>
<td>Event WLAN Kerberos authentication failed message</td>
</tr>
<tr>
<td>kerberos-wlan-success</td>
<td>Event WLAN Kerberos authentication success message</td>
</tr>
<tr>
<td>kerberos-wlan-timeout</td>
<td>Event Kerberos authentication timed out message</td>
</tr>
<tr>
<td>move-operation-success</td>
<td>Event move operation success message</td>
</tr>
<tr>
<td>neighbor-denied-assoc</td>
<td>Event neighbor denied association message</td>
</tr>
<tr>
<td>tkip-cntrmes-end</td>
<td>Event TKIP countermeasures ended message</td>
</tr>
<tr>
<td>tkip-cntrmes-start</td>
<td>Event TKIP countermeasures initiated message</td>
</tr>
<tr>
<td>tkip-mic-fail-report</td>
<td>Event TKIP MIC failure report</td>
</tr>
<tr>
<td>tkip-mic-failure</td>
<td>Event TKIP MIC check failed message</td>
</tr>
<tr>
<td>voice-call-completed</td>
<td>Event voice call completed message</td>
</tr>
<tr>
<td>voice-call-established</td>
<td>Event voice call established message</td>
</tr>
<tr>
<td>Contd..</td>
<td></td>
</tr>
<tr>
<td>&lt;event-type&gt;</td>
<td>&lt;event-name&gt;</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>dot1x</td>
<td>Enables and configures the logging of 802.1X authentication related event messages</td>
</tr>
<tr>
<td></td>
<td>• dot1x-failed – Event EAP authentication failure message</td>
</tr>
<tr>
<td></td>
<td>• dot1x-success – Event dot1x-success message</td>
</tr>
<tr>
<td>fwu</td>
<td>Enables and configures the logging of firmware update (fwu) related event messages</td>
</tr>
<tr>
<td></td>
<td>• fwuaborted – Event fwu aborted message</td>
</tr>
<tr>
<td></td>
<td>• fwubadconfig – Event fwu aborted due to bad config message</td>
</tr>
<tr>
<td></td>
<td>• fwucorruptedfile – Event fwu aborted due to corrupted file message</td>
</tr>
<tr>
<td></td>
<td>• fwucouldntgetfile – Event fwu aborted because the system could not get file message</td>
</tr>
<tr>
<td></td>
<td>• fwudone – Event fwu done message</td>
</tr>
<tr>
<td></td>
<td>• fwufileundefined – Event fwu aborted due to file undefined message</td>
</tr>
<tr>
<td></td>
<td>• fwunoneed – Event fwu no need message</td>
</tr>
<tr>
<td></td>
<td>• fwuprodmismatch – Event fwu aborted due to product mismatch message</td>
</tr>
<tr>
<td></td>
<td>• fwuserverundefined – Event fwu aborted due to server undefined message</td>
</tr>
<tr>
<td></td>
<td>• fwuserverunreachable – Event fwu aborted due to server unreachable message</td>
</tr>
<tr>
<td></td>
<td>• fwusignmismatch – Event fwu aborted due to signature mismatch message</td>
</tr>
<tr>
<td></td>
<td>• fwusyserr – Event fwu aborted due to system error message</td>
</tr>
<tr>
<td></td>
<td>• fwuunsupportedhw – Event fwu aborted due to unsupported hardware message</td>
</tr>
<tr>
<td></td>
<td>• fwuunsupportedmodelnum – Event fwu aborted due to unsupported FIPS model number message</td>
</tr>
<tr>
<td></td>
<td>• fwuvemismatch – Event fwu aborted due to version mismatch message</td>
</tr>
<tr>
<td>isdn</td>
<td>Enables and configures the logging of file Integrated Service Digital Network (ISDN) module related event messages</td>
</tr>
<tr>
<td></td>
<td>• isdn-alert – Event ISDN alert message</td>
</tr>
<tr>
<td></td>
<td>• isdn-crit – Event ISDN critical message</td>
</tr>
<tr>
<td></td>
<td>• isdn-debug – Event ISDN debug message</td>
</tr>
<tr>
<td></td>
<td>• isdn-emerg – Event ISDN emergency message</td>
</tr>
<tr>
<td></td>
<td>• isdn-err – Event ISDN error message</td>
</tr>
<tr>
<td></td>
<td>• isdn-info – Event ISDN info message</td>
</tr>
<tr>
<td></td>
<td>• isdn-notice – Event ISDN notice message</td>
</tr>
<tr>
<td></td>
<td>• isdn-warn – Event ISDN warning message</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Enables and configures the logging of L2TPv3 related event messages</td>
</tr>
<tr>
<td></td>
<td>• l2tpv3-tunnel-down – Event L2TPv3 tunnel down message</td>
</tr>
<tr>
<td></td>
<td>• l2tpv3-tunnel-up – Event L2TPv3 tunnel up message</td>
</tr>
<tr>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>licmgr</td>
<td>Enables and configures the logging of license manager module related event messages</td>
</tr>
<tr>
<td></td>
<td>• lic-installed-count – Event total number of license installed count message</td>
</tr>
<tr>
<td></td>
<td>• lic-installed-default – Event default license installation message</td>
</tr>
<tr>
<td></td>
<td>• lic-installed – Event license installed message</td>
</tr>
<tr>
<td></td>
<td>• lic-invalid – Event license installation failed message</td>
</tr>
<tr>
<td></td>
<td>• lic-removed – Event license removed message</td>
</tr>
<tr>
<td>mgmt</td>
<td>Enables and configures the logging of management services module related event messages</td>
</tr>
<tr>
<td></td>
<td>• log-http-init – Event Web server started</td>
</tr>
<tr>
<td></td>
<td>• log-http-local-start – Event Web server started in local mode</td>
</tr>
<tr>
<td></td>
<td>• log-http-start – Event Web server started in external mode</td>
</tr>
<tr>
<td></td>
<td>• log-https-start – Event secure Web server started</td>
</tr>
<tr>
<td></td>
<td>• log-https-wait – Event waiting for Web server to start</td>
</tr>
<tr>
<td></td>
<td>• log-key-deleted – Event RSA key associated with SSH is deleted</td>
</tr>
<tr>
<td></td>
<td>• log-key-restored – Event RSA key associated with SSH is added</td>
</tr>
<tr>
<td></td>
<td>• log-trustpoint-deleted – Event trustpoint associated with HTTPS is deleted</td>
</tr>
<tr>
<td>mesh</td>
<td>Enables and configures the logging of mesh module related event messages</td>
</tr>
<tr>
<td></td>
<td>• mesh-link-down – Event mesh link down message</td>
</tr>
<tr>
<td></td>
<td>• mesh-link-up – Event mesh link up message</td>
</tr>
<tr>
<td></td>
<td>• meshpoint-down – Event meshpoint down message</td>
</tr>
<tr>
<td></td>
<td>• meshpoint-loop-prevent-off – Event meshpoint loop prevent off message</td>
</tr>
<tr>
<td></td>
<td>• meshpoint-loop-prevent-on – Event meshpoint loop prevent on message</td>
</tr>
<tr>
<td></td>
<td>• meshpoint-path-change – Event meshpoint-path-change message</td>
</tr>
<tr>
<td></td>
<td>• meshpoint-root-change – Event meshpoint-root-change message</td>
</tr>
<tr>
<td></td>
<td>• meshpoint-up – Event meshpoint up message</td>
</tr>
<tr>
<td>nsm</td>
<td>Enables and configures the logging of Network Service Module (NSM) related event messages</td>
</tr>
<tr>
<td></td>
<td>• dhcpc-err – Event DHCP certification error message</td>
</tr>
<tr>
<td></td>
<td>• dhcpdefrt – Event DHCP defrt message</td>
</tr>
<tr>
<td></td>
<td>• dhcpip – Event DHCP IP message</td>
</tr>
<tr>
<td></td>
<td>• dhcpipch – Event DHCP IP change message</td>
</tr>
<tr>
<td></td>
<td>• dhcpipnoadd – Event DHCP IP overlaps static IP address message</td>
</tr>
<tr>
<td></td>
<td>• dhcplsex – Event DHCP lease expiry message</td>
</tr>
<tr>
<td></td>
<td>• dhcpnak – Event DHCP server returned DHCP NAK response</td>
</tr>
<tr>
<td></td>
<td>• dhcpnodef – Event interface no default route message</td>
</tr>
<tr>
<td></td>
<td>• if-failback – Event interface failback message</td>
</tr>
<tr>
<td></td>
<td>• if-failover – Event interface failover message</td>
</tr>
<tr>
<td></td>
<td>• ifdown – Event interface down message</td>
</tr>
<tr>
<td></td>
<td>• ifipcfg – Event interface IP config message</td>
</tr>
<tr>
<td></td>
<td>• ifup – Event interface up message</td>
</tr>
<tr>
<td></td>
<td>• nsm-ntp – Event translate host name message</td>
</tr>
<tr>
<td></td>
<td>• ntp-start – Event NTP server start message</td>
</tr>
<tr>
<td></td>
<td>• ntp-stop – Event NTP server stop message</td>
</tr>
<tr>
<td><code>&lt;event-type&gt;</code></td>
<td><code>&lt;event-name&gt;</code></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| pm            | Enables and configures the logging of process monitor module related event messages  
|               | - procid – Event proc ID message  
|               | - procmaxrstrt – Event proc max restart message  
|               | - procnoresp – Event proc no response message  
|               | - procrstrt – Event proc restart message  
|               | - procstart – Event proc start message  
|               | - procsysrstrt – Event proc system restart message  
|               | - startupcomplete – Event startup complete message  |
| radconf       | Enables and configures the logging of RADIUS configuration daemon related event messages  
|               | - could-not-stop-radius – Event could not stop RADIUS server message  
|               | - radiusdstart – Event RADIUS server started message  
|               | - radiusdstop – Event RADIUS server stopped message  |
| radio         | Enables and configures the logging of radio module related event messages  
|               | - acs-scan-complete – Event ACS scan completed  
|               | - acs-scan-started – Event ACS scan started  
|               | - channel-country-mismatch – Event channel and country of operation mismatch message  
|               | - radar-det-info – Detected radar info message  
|               | - radar-detected – Event radar detected message  
|               | - radar-scan-completed – Event radar scan completed message  
|               | - radar-scan-started – Event radar scan started message  
|               | - radio-antenna-error – Event invalid antenna type on this radio message  
|               | - radio-antenna-setting – Event antenna type setting on this radio message  
|               | - radio-state-change – Event radio state change message  
|               | - resume-home-channel – Event resume home channel message  |
| rasst         | Enables and configures the logging of roaming assist module related event message  |
| smrt          | Enables and configures the logging of SMART RF module related event messages  
|               | - calibration-done – Event calibration done message  
|               | - calibration-started – Event calibration started message  
|               | - channel-change – Event channel change message  
|               | - config-cleared – Configuration cleared event message  
|               | - cov-hole-recovery – Event coverage hole recovery message  
|               | - cov-hole-recovery-done – Event coverage hole recovery done message  
|               | - interference-recovery – Event interference recovery message  
|               | - neighbor-recovery – Event neighbor recovery message  
|               | - power-adjustment – Event power adjustment message  
<p>|               | - root-recovery – Event meshpoint root recovery message  |</p>
<table>
<thead>
<tr>
<th>&lt;event-type&gt;</th>
<th>&lt;event-name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtpnot</td>
<td>Enables and configures the logging of SMTP module related event messages</td>
</tr>
<tr>
<td></td>
<td>• cfg – Event cfg message</td>
</tr>
<tr>
<td></td>
<td>• cfginc – Event cfg inc message</td>
</tr>
<tr>
<td></td>
<td>• net – Event net message</td>
</tr>
<tr>
<td></td>
<td>• proto – Event proto message</td>
</tr>
<tr>
<td></td>
<td>• smtpauth – Event SMTP authentication message</td>
</tr>
<tr>
<td></td>
<td>• smtperr – Event SMTP error message</td>
</tr>
<tr>
<td></td>
<td>• smtpinfo – Event SMTP information message</td>
</tr>
<tr>
<td>system</td>
<td>Enables and configures the logging of system module related event messages</td>
</tr>
<tr>
<td></td>
<td>• clock-reset – Event clock reset message</td>
</tr>
<tr>
<td></td>
<td>• cold-start – Event cold start message</td>
</tr>
<tr>
<td></td>
<td>• config-commit – Event configuration commit message</td>
</tr>
<tr>
<td></td>
<td>• config-revision – Event config-revision done message</td>
</tr>
<tr>
<td></td>
<td>• devup-rfd-fail – Event device-upgrade failed on rf-domain manager managed devices message</td>
</tr>
<tr>
<td></td>
<td>• guest-user-exp – Event guest user purging message</td>
</tr>
<tr>
<td></td>
<td>• http-err – Event Web server did not start message</td>
</tr>
<tr>
<td></td>
<td>• login – Event successful login message</td>
</tr>
<tr>
<td></td>
<td>• login-fail – Event login fail message. Occurs when user authentication fails.</td>
</tr>
<tr>
<td></td>
<td>• login-fail-access – Event login fail access message. Occurs in case of access violation.</td>
</tr>
<tr>
<td></td>
<td>• login-fail-bad-role – Event login fail bad role message. Occurs when user uses an invalid role to logon.</td>
</tr>
<tr>
<td></td>
<td>• logout – Event logout message</td>
</tr>
<tr>
<td></td>
<td>• maat-light – Event action on Research in Motion (RIM) radio(s) from the Maat light module</td>
</tr>
<tr>
<td></td>
<td>• panic – Event panic message</td>
</tr>
<tr>
<td></td>
<td>• periodic-heart-beat – Event periodic heart beat message</td>
</tr>
<tr>
<td></td>
<td>• proctstop – Event proc stop message</td>
</tr>
<tr>
<td></td>
<td>• server-unreachable – Event server-unreachable message</td>
</tr>
<tr>
<td></td>
<td>• system-autoup-disable – Event system autoup disable message</td>
</tr>
<tr>
<td></td>
<td>• system-autoup-enable – Event system autoup enable message</td>
</tr>
<tr>
<td></td>
<td>• t5-config-error – Event t5-config-error message</td>
</tr>
<tr>
<td></td>
<td>• ui-user-auth-fail – Event user authentication fail message</td>
</tr>
<tr>
<td></td>
<td>• ui-user-auth-success – Event user authentication success message</td>
</tr>
<tr>
<td></td>
<td>• warm-start – Event warm start message</td>
</tr>
<tr>
<td></td>
<td>• warm-start-recover – Event recovery from warm start message</td>
</tr>
<tr>
<td><code>&lt;event-type&gt;</code></td>
<td><code>&lt;event-name&gt;</code></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| **test**      | Enables and configures the logging of the test module related event messages  
• testalert – Event test alert message  
• testargs – Event test arguments message  
• testcrit – Event test critical message  
• testdebug – Event test debug message  
• testemerg – Event test emergency message  
• testerr – Event test error message  
• testinfo – Event test information message  
• testnotice – Event test notice message  
• testwarn – Event test warning message |
| **vrrp**      | Enables and configures the logging of *Virtual Router Redundancy Protocol* (VRRP) related event messages  
• vrrp-monitor-change – Event VRRP monitor link state change message  
• vrrp-state-change – Event VRRP state transition message  
• vrrp-vip-subnet-mismatch – Event VRRP IP not overlapping with an interface addresses message |
| **wips**      | Enables and configures the logging of the Wireless IPS module related event messages  
• air-termination-active – Event air termination active message  
• air-termination-ended – Event air termination ended message  
• air-termination-inactive – Event air termination inactive message  
• air-termination-initiated – Event air termination initiated message  
• rogue-ap-active – Event rogue AP active message  
• rogue-ap-inactive – Event rogue AP inactive message  
• unsanctioned-ap-active – Event unsanctioned AP active message  
• unsanctioned-ap-inactive – Event unsanctioned AP inactive message  
• unsanctioned-ap-status-change – Event unsanctioned AP changed state message  
• wips-client-blacklisted – Event WIPS client blacklisted message  
• wips-client-rem-blacklist – Event WIPS client rem blacklist message  
• wips-event – Event WIPS event triggered message |
| **email**     | Sends e-mail notifications to a pre configured e-mail ID |
| **forward-to-switch** | Forwards the messages to an external server |
| **snmp**      | Logs an SNMP event |
| **syslog**    | Logs an event to syslog |
| **default**   | Performs the default action for the event |
| **off**       | Switches the event off, when the event happens, and no action is performed |
| **on**        | Switches the event on, when the event happens, and the configured action is taken |
Examples

```
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#event aaa radius-discon-msg email on forward-to-switch default smtp default syslog default
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#
```

```
rfs7000-37FABE(config-event-system-policy-testpolicy)#show context event-system-policy test
   event aaa radius-discon-msg email on
rfs7000-37FABE(config-event-system-policy-testpolicy)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets or disables event monitoring</td>
</tr>
</tbody>
</table>
4.1.40.2.2 no

*event-system-policy-mode commands*

Negates an event monitoring configuration

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no event <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog]
  [default|on|off]
```

**Parameters**

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes event monitoring and message forwarding activity based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> The system stops network monitoring for the occurrence of the specified event and no notification is sent if the event occurs.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-event-system-policy-TestPolicy)#event ap adopted syslog default
rfs7000-37FABE(config-event-system-policy-TestPolicy)#no event ap adopted syslog
```

**Related Commands**

- `event` Configures the action taken for each event
### 4.1.41 ex3500

The following table lists EX3500 time-range configuration mode commands. It also provides links to other EX3500 related configuration modes:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ex3500</code></td>
<td>Creates an EX3500 time range list and enters its configuration mode</td>
<td>page 4-168</td>
</tr>
<tr>
<td><code>ex3500-time-range-config-mode</code></td>
<td>Summarizes EX3500 time range list configuration mode commands</td>
<td>page 4-169</td>
</tr>
<tr>
<td><code>ex3500-management-policy</code></td>
<td>Creates an EX3500 management policy and enters its configuration mode</td>
<td>page 4-174</td>
</tr>
<tr>
<td><code>ex3500-qos-class-map-policy</code></td>
<td>Creates an EX3500 QoS class map policy and enters its configuration mode</td>
<td>page 4-192</td>
</tr>
<tr>
<td><code>ex3500-qos-policy-map</code></td>
<td>Creates an EX3500 QoS policy map and enters its configuration mode</td>
<td>page 4-200</td>
</tr>
<tr>
<td><code>ex3524</code></td>
<td>Adds a EX3524 switch to the network</td>
<td>page 4-214</td>
</tr>
<tr>
<td><code>ex3548</code></td>
<td>Adds a EX3548 switch to the network</td>
<td>page 4-216</td>
</tr>
</tbody>
</table>
4.1.41.1 ex3500

`ex3500`

Creates an EX3500 time range list and enters its configuration mode.

An EX3500 time range list consists of a set of periodic and absolute time range rules. Periodic time ranges recur periodically at specified time periods, such as daily, weekly, weekends, weekdays, and on specific week days, for example on every successive Mondays. Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period (the starting and ending days and time are fixed).

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four Small Form Factor Pluggable (SFP) transceiver slots for fiber connectivity. The EX3500 series switch can adopt to a WiNG NOC controller and be managed by it. The EX3500 time range values configured here are used in EX3500 MAC ACL firewall rules that filters an EX3500's incoming and outgoing traffic. For more information on creating EX3500 MAC ACL rules, see `ex3500` and `access-group`.

Supported in the following platforms:

- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

`ex3500 time-range <TIME-RANGE-NAME>`

**Parameters**

- `ex3500 time-range <TIME-RANGE-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ex3500 time-range &lt;TIME-RANGE-NAME&gt;</code></td>
<td>Configures EX3500 time range list and enters its configuration mode</td>
</tr>
<tr>
<td><code>&lt;TIME-RANGE-NAME&gt;</code></td>
<td>Enter a name for this EX3500 time range. If the time range does not exist, it is created.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
nx9500-6C8809(config)#ex3500 time-range EX3500_TimeRange_02
nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#?
```

EX3500 Time Range Configuration commands:

- `absolute`  Absolute time and date
- `no`        Negate a command or set its defaults
- `periodic`  Periodic time and date
- `clrscr`    Clears the display screen
- `commit`    Commit all changes made in this session
- `do`        Run commands from Exec mode
- `end`       End current mode and change to EXEC mode
- `exit`      End current mode and down to previous mode
- `help`      Description of the interactive help system
- `revert`    Revert changes
- `service`   Service Commands
- `show`      Show running system information
- `write`     Write running configuration to memory or terminal

```bash
nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#
```

**Related Commands**

- `no`          Removes this EX3500 time range list
4.1.41.2 ex3500-time-range-config-mode commands

ex3500

The following table summarizes EX3500 time-range configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>absolute</td>
<td>Configures an absolute time range rule for this EX3500 time range list</td>
<td>page 4-170</td>
</tr>
<tr>
<td>periodic</td>
<td>Configures a periodic time range rule for this EX3500 time range list</td>
<td>page 4-171</td>
</tr>
<tr>
<td>no</td>
<td>Removes this EX3500 time range list settings</td>
<td>page 4-173</td>
</tr>
</tbody>
</table>
### 4.1.41.2.1 absolute

**ex3500-time-range-config-mode commands**

Configures an absolute time range rule for this EX3500 time range list

Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```plaintext
absolute start <0-23> <0-59> <1-31> <MONTH> <2013-2037> {end <0-23> <0-59> <1-31> <MONTH> <2013-2037>}
```

**Parameters**
- `absolute start <0-23> <0-59> <1-31> <MONTH> <2013-2037> {end <0-23> <0-59> <1-31> <MONTH> <2013-2037>}`

<table>
<thead>
<tr>
<th>absolute</th>
<th>Configures an absolute time range rule settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>start &lt;0-23&gt; &lt;0-59&gt; &lt;1-31&gt; &lt;MONTH&gt; &lt;2013-2037&gt;</td>
<td>Configures the start day and time settings</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-23&gt; – Specify the start time from 0 - 23 hours.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-59&gt; – Specify the start time from 0 - 59 minutes.</td>
</tr>
<tr>
<td><strong>Note:</strong> For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;1-31&gt; – Specify the day of month from 1 - 31 when the time range starts.</td>
</tr>
<tr>
<td></td>
<td>• &lt;MONTH&gt; – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September.</td>
</tr>
<tr>
<td></td>
<td>• &lt;2013-2037&gt; – Specify the year from 2013 - 2037.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>end &lt;0-23&gt; &lt;0-59&gt; &lt;1-31&gt; &lt;MONTH&gt; &lt;2013-2037&gt;</th>
<th>Optional. Configures the end day and time settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;0-23&gt; – Specify the end time from 0 - 23 hours.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-59&gt; – Specify the end time from 0 - 59 minutes.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-31&gt; – Specify the day of month from 1 - 31 when the time range ends.</td>
</tr>
<tr>
<td></td>
<td>• &lt;MONTH&gt; – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September.</td>
</tr>
<tr>
<td></td>
<td>• &lt;2013-2037&gt; – Specify the year from 2013 - 2037.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#absolute start 1 0 1 june 2015 end 1 0 30 june 2016
```

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context ex3500 time-range EX3500-TimeRange-01
  absolute start 1 0 1 june 2015 end 1 0 30 june 2016
```

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#af
```

**Related Commands**

| no | Removes this absolute time range rule from the EX3500 time range list |
4.1.41.2.2 periodic

**ex3500-time-range-config-mode commands**

Configures a periodic time range rule for this EX3500 time range list

Periodic time ranges are configured to recur based on periodicity such as daily, weekly, weekends, weekdays, and on specific week days, such as on every successive Sunday.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```plaintext
periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend] <0-23> <0-59> to [<023> <0-59]|daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend] <0-23> <0-59> rule-precedence <1-7>
```

**Parameters**

- **periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend]**
  Configures this periodic time range’s start day. The options are:
  - daily
  - friday
  - monday
  - saturday
  - sunday
  - thursday
  - tuesday
  - wednesday
  - weekdays
  - weekend

- **<0-23> <0-59>**
  After specifying the start day, specify the start time in hours (24 hours format) and minutes
  - **<0-23>** – Specify the start time from 0 - 23 hours.
  - **<0-59>** – Specify the start time from 0 - 59 minutes.

  For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day.

- **to [<023> <0-59]|daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend]**
  Configures this periodic time range’s end day. This is the day when the time range ends.
  The options available changes depending on the **start day** configured. The options are:
  - **<0-23> <0-59>** – Select this option to end the time range on the same day as it starts.
    Specify the end hour from 0 - 23 hours and the minutes from 0 - 59 minutes.
  - daily – Select this option if the time range starts and ends every day at a specified time
  - friday – Select this option if the time range ends on Fridays
  - monady – Select this option if the time range ends on Mondays
  - saturday – Select this option if the time range ends on Saturdays
  - sunday – Select this option if the time range ends on Sundays

Contd..
### Examples

- **nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#periodic daily 1 10 to daily 23 10 rule-precedence 1**

- **nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context ex3500 time-range EX3500-TimeRange-01 periodic daily 1 10 to daily 23 10 rule-precedence 1 absolute start 1 0 1 june 2015 end 1 0 30 june 2016**

### Related Commands

- **no**  
  Removes this periodic time range rule from the EX3500 time range list
4.1.41.2.3 no

- **ex3500-time-range-config-mode commands**

Removes this EX3500 time range list settings

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

no [absolute|periodic]

no absolute

no periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend] <0-23> <0-59> to [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend]

**Parameters**

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes this EX3500 time range list settings based on the parameters passed</th>
</tr>
</thead>
</table>

**Examples**

```plaintext
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context ex3500 time-range EX3500-TimeRange-01
  periodic daily 1 10 to daily 23 10 rule-precedence 1
  absolute start 1 0 1 june 2015 end 1 0 30 june 2016

nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#no periodic daily 1 10 to daily 23 10 rule-precedence 1

nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context ex3500 time-range EX3500-TimeRange-01
  absolute start 1 0 1 june 2015 end 1 0 30 june 2016
```
### 4.1.42 ex3500-management-policy

> **Global Configuration Commands**

The following table lists EX3500 management policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ex3500-management-policy</code></td>
<td>Creates an EX3500 management policy and enters its configuration mode</td>
<td>page 4-175</td>
</tr>
<tr>
<td><code>ex3500-management-policy config commands</code></td>
<td>Summarizes EX3500 management policy configuration mode commands</td>
<td>page 4-177</td>
</tr>
<tr>
<td><code>ex3500</code></td>
<td>Creates an EX3500 time range list and enters its configuration mode</td>
<td>page 4-167</td>
</tr>
<tr>
<td><code>ex3500-qos-class-map-policy</code></td>
<td>Creates an EX3500 QoS class map policy and enters its configuration mode</td>
<td>page 4-192</td>
</tr>
<tr>
<td><code>ex3500-qos-policy-map</code></td>
<td>Creates an EX3500 QoS policy map and enters its configuration mode</td>
<td>page 4-200</td>
</tr>
<tr>
<td><code>ex3524</code></td>
<td>Adds a EX3524 switch to the network</td>
<td>page 4-214</td>
</tr>
<tr>
<td><code>ex3548</code></td>
<td>Adds a EX3548 switch to the network</td>
<td>page 4-216</td>
</tr>
</tbody>
</table>
4.1.42.1 ex3500-management-policy

Creates an EX3500 management policy and enters its configuration mode. Once configured and applied on a
EX3500 switch, the management policy controls access to the switch from management stations using SNMP.
The EX3500 management policy is either applied:

- Individually on an adopted EX3500 series switch (in the device configuration mode), or
- To a EX3524 and/or EX3548 profile, which is then applied to an adopted EX3500 series switch.

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-
BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the
IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent
that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP
Web agent and CLI, which in spite of being different from that of the WING operating system provides WING
controllers PoE and port management resources.

Going forward NX9500, NX7500, NX6500, NX4500 WING managed series service platforms and WING VMs can
discover, adopt, and partially manage EX3500 series Ethernet switches without modifying the proprietary
operating system running the EX3500 switches. The WING service platforms utilize standardized WING interfaces
to push configuration files to the EX3500 switches, and maintain a translation layer, understood by the EX3500
switch, for statistics retrieval.

WING can partially manage an EX3500 without using DHCP option 193, provided the EX3500 is directly
configured to specify the IPv4 addresses of potential WING adopters. To identify the potential WING adopter, in
the EX3500’s device configuration mode specify the adopter’s IPv4 address using the
controller > host > <IP-ADDRESS> command. WING service platforms leave the proprietary operating system
running the EX3500 switches unmodified, and partially manage them utilizing standardized WING interfaces.
WING service platforms use a translation layer to communicate with the EX3500.

Supported in the following platforms:

- Wireless Controller — RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9500

Syntax

ex3500-management-policy <POLICY-NAME>

Parameters

- ex3500-management-policy <POLICY-NAME>

| <POLICY-NAME> | Specify the EX3500 management policy name. If the policy does not exist, it is created. |

Examples

nx9500-6C8809(config)#ex3500-management-policy test
nx9500-6C8809(config-ex3500-management-policy-test)#?

EX3500 Management Mode commands:

- enable: Modifies enable password parameters
- http: Hyper Text Terminal Protocol (HTTP)
- memory: Memory utilization
- no: Negate a command or set its defaults
- process-cpu: Process-cpu utilization
- snmp-server: Enable SNMP server configuration
- ssh: Secure Shell server connections
- username: Login TACACS server port
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
### Service Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

nx9500-6C8809(config-ex3500-management-policy-test)#

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes this EX3500 management policy</td>
</tr>
</tbody>
</table>
4.1.42.2 ex3500-management-policy config commands

The following table summarizes EX3500 management policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Configures an executive password for this EX3500 management policy</td>
<td>page 4-178</td>
</tr>
<tr>
<td>http</td>
<td>Configures the HTTP server settings used to authenticate HTTP connection</td>
<td>page 4-179</td>
</tr>
<tr>
<td></td>
<td>to a EX3500 switch</td>
<td></td>
</tr>
<tr>
<td>memory</td>
<td>Configures the EX3500’s memory utilization rising (upper) and falling (lower)</td>
<td>page 4-180</td>
</tr>
<tr>
<td></td>
<td>threshold values</td>
<td></td>
</tr>
<tr>
<td>process-cpu</td>
<td>Configures the EX3500’s CPU (processor) utilization rising (upper) and</td>
<td>page 4-181</td>
</tr>
<tr>
<td></td>
<td>falling (lower) threshold values</td>
<td></td>
</tr>
<tr>
<td>snmp-server</td>
<td>Configures Simple Network Management Protocol (SNMP) server settings.</td>
<td>page 4-182</td>
</tr>
<tr>
<td></td>
<td>Once configured and applied on a EX3500 switch, the management policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>controls access to the switch from management stations using SNMP.</td>
<td></td>
</tr>
<tr>
<td>ssh</td>
<td>Configures the SSH server settings used to authenticate Secure Shell (SSH)</td>
<td>page 4-188</td>
</tr>
<tr>
<td></td>
<td>connection to a EX3500 switch</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>Configures a EX3500 switch user settings</td>
<td>page 4-189</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts this EX3500 management policy settings</td>
<td>page 4-190</td>
</tr>
</tbody>
</table>
4.1.42.2.1 enable

ex3500-management-policy config commands

Configures an executive password for this EX3500 management policy

Each EX3500 management policy can have a unique executive password with its own privilege level assigned. Utilize these passwords as specific EX3500 management sessions require priority over others.

Supported in the following platforms:

- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

```
enable password [0|7|level]
```

```
enable password [0|7] <PASSWORD>
```

```
enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]
```

Parameters

- `enable password [0|7] <PASSWORD>`

- `enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]`

Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#enable password level 3 7 12345678901020304050607080929291
nx9500-6C8809(config-ex3500-management-policy-test)#show context ex3500-management-policy-test enable password level 3 7 12345678901020304050607080929291 snmp-server notify-filter 1 remote 127.0.0.1
```

Related Commands

| no |
| Removes a executive password from this EX3500 management policy |
4.1.42.2.2  http

Configures the HTTP server settings used to authenticate HTTP connection to a EX3500 switch.

Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling un-used and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax
http [port <1-65535>|secure-port <1-65535>|secure-server|server]

Parameters
- http [port <1-65535>|secure-port <1-65535>|secure-server|server]

<table>
<thead>
<tr>
<th>http</th>
<th>Configures following HTTP settings: port, secure-port, secure-server, and server</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Configures the HTTP port number. This is the port used to connect to the HTTP server.</td>
</tr>
<tr>
<td>secure-port &lt;1-65535&gt;</td>
<td>Enables secure HTTP connection over a designated secure port. Ensure that the HTTP server is enabled before specifying the secure-server port.</td>
</tr>
<tr>
<td>secure-server</td>
<td>Enables HTTP secure server. This option is disabled by default.</td>
</tr>
<tr>
<td>server</td>
<td>Enables HTTP server. This option is enabled by default. Consequently, HTTP management access is allowed by default.</td>
</tr>
</tbody>
</table>

Examples
nx9500-6C8809(config-ex3500-management-policy-test)#http secure-server

nx9500-6C8809(config-ex3500-management-policy-test)#show context ex3500-management-policy test
http secure-server
enable password level 3 7 12345678901020304050607080929291
snmp-server notify-filter 1 remote 127.0.0.1

Related Commands
- **no**  Reverts to default HTTP server settings (HTTP server enabled, HTTP port 80)
4.12.2.3 memory

ex3500-management-policy config commands

Configures the EX3500’s memory utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the memory utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500’s memory and CPU utilization’s upper and lower thresholds, you can avoid over utilization of the EX3500’s processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

Supported in the following platforms:
  • Wireless Controller — RFS7000
  • Service Platforms — NX7500, NX9500

Syntax
memory [falling-threshold|rising-threshold] <1-100>

Parameters
- memory [falling-threshold|rising-threshold] <1-100>

| memory | Configures the EX3500’s memory utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded. |
| falling-threshold <1-100> | Configures the falling threshold for the EX3500 memory utilization
  • <1-100> – Specify the falling threshold as a percentage from 1 - 100. The default is 70%. |
| rising-threshold <1-100> | Configures the rising threshold for the EX3500’s memory utilization
  • <1-100> – Specify the rising threshold as a percentage from 1 - 100. The default is 90%. |

Examples
nx9500-6C8809(config-ex3500-management-policy-test)#memory falling-threshold 50
nx9500-6C8809(config-ex3500-management-policy-test)#memory rising-threshold 95
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
  http secure-server
  enable password level 3 7 1234567890120304050607080929291
  snmp-server notify-filter 1 remote 127.0.0.1
  memory falling-threshold 50
  memory rising-threshold 95

Related Commands

| no | Reverts the memory utilization’s falling-threshold and/or rising threshold to 70% and 90% respectively |
4.1.42.2.4  process-cpu

Configures the EX3500’s CPU (processor) utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the CPU utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500’s memory and CPU utilization’s upper and lower thresholds, you can avoid over utilization of the EX3500’s processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

```
process-cpu [falling-threshold|rising-threshold] <1-100>
```

Parameters

- `process-cpu [falling-threshold|rising-threshold] <1-100>`

<table>
<thead>
<tr>
<th>process-cpu</th>
<th>Configures the EX3500’s CPU utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded.</th>
</tr>
</thead>
</table>
| falling-threshold <1-100> | Configures the falling threshold for the EX3500’s CPU utilization  
  - `<1-100>` – Specify the falling threshold as a percentage from 1 - 100. The default is 70%. |
| rising-threshold <1-100> | Configures the rising threshold for the EX3500’s CPU utilization  
  - `<1-100>` – Specify the rising threshold as a percentage from 1 - 100. The default is 90%. |

Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#process-cpu falling-threshold 60
nx9500-6C8809(config-ex3500-management-policy-test)#process-cpu rising-threshold 80
```

```
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
  http secure-server
  enable password level 3 7 1234567890120304050607080929291
  snmp-server notify-filter 1 remote 127.0.0.1
  memory falling-threshold 50
  memory rising-threshold 95
  process-cpu falling-threshold 60
  process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#
```

Related Commands

- `no` Reverts the CPU utilization’s falling-threshold and/or rising threshold to 70% and 90% respectively
4.1.42.2.5 snmp-server

**ex3500-management-policy config commands**

Configures Simple Network Management Protocol (SNMP) server settings. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP.

SNMP is an application layer protocol that facilitates the exchange of management information between the management stations and a managed EX3500 switch. SNMP-enabled devices listen on port 162 (by default) for SNMP packets from the management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system's performance and other parameters.

Supported in the following platforms:

- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```
snmp-server {community|contact|enable|engine-id|group|host|location|notify-filter|
user|view}

snmp-server {community <STRING> {ro|rw}}

snmp-server {contact <NAME>}

snmp-server {enable traps {authentication|link-up-down}}

snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]} 

snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]] {notify <WORD>|read <WORD>|write <WORD>}}

snmp-server {host <IP> [inform]} 

{udp-port <1-65535>}

snmp-server {host <IP> inform [retry <0-255>|timeout <0-2147483647>]} <STRING>

version [v2c|v3 [auth|noauth|priv]] {udp-port <1-65535>}

snmp-server {location <WORD>}

snmp-server {notify-filter <WORD> remote <IP>}

snmp-server {user <USER-NAME> <GROUP-NAME> [remote-host|v1|v2c|v3]}

snmp-server {user <USER-NAME> <GROUP-NAME> remote-host <IP> v3 [auth|encrypted auth]

[md5|sha] <WORD> [priv [3des|aes128|aes192|aes256|des56] <WORD>]

snmp-server {user <USER-NAME> <GROUP-NAME> [v1|v2c|v3]}

snmp-server {view <VIEW-NAME> <OID-TREE-STRING> [excluded|included]}

**Parameters**

- **snmp-server {community <STRING> {ro|rw}}**

| snmp-server community <STRING> {ro|rw} | Configures SNMP-server related settings |
|----------------------------------------|----------------------------------------|
| • community – Optional. Configures an SNMP community access string used to authorize management access by clients using SNMP v1, v2c, or v3 |
| • <STRING> – Specify the SNMP community access string (should not exceed 32 characters). |

Contd..
### SNMP Configuration Commands

**snmp-server contact <NAME>**

Configures SNMP-server related settings
- contact – Optional. Configures the system’s contact information
  - <NAME> – Specify the contact person's name (should not exceed 255 characters).

**snmp-server enable traps {authentication|link-up-down}**

Configures SNMP-server related settings
- enable traps – Optional. Enables the EX3500 switch to send following SNMP traps or notifications:
  - authentication – Optional. Enables SNMP authentication trap. This option is disabled by default.
  - link-up-down – Optional. Enables SNMP link up and link down traps. This option is disabled by default.

**snmp-server engine-id [local <WORD> | remote <IP> <WORD>]**

Configures SNMP-server related settings
- engine-id – Optional. Configures an identification string for the SNMPv3 engine. The SNMP engine is an independent SNMP agent residing either on the logged switch or on a remote device. It prevents message replay, delay, and redirection. In SNMPv3, the engine ID in combination with user passwords generates the security keys that is used for SNMPv3 packet authentication and encryption.
  - local – Configures the SNMP engine on the logged switch
    - <WORD> – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).
  - remote <IP> <WORD> – Configures a remote device as the SNMP engine
    - <IP> – Specify the remote device’s IP address.
    - <WORD> – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).

Configure the remote engine ID when using SNMPv3 informs. The remote ID configured here is used to generate the security digest for authentication and encryption of packets exchanged between the switch and the and the remote host user. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it.
### snmp-server group <GROUP-NAME>

Configures SNMP-server related settings

- **group** – Optional. Configures an SNMP user group, mapping SNMP users to SNMP views
  - `<GROUP-NAME>` – Specify the SNMP group name (should not exceed 32 characters).

- **[v1|v2c|v3 [auth|noauth|priv]]**
  - Configures the SNMP version used for authentication by this user group
  - `v1` – Configures the SNMP version as v1.
  - `v2c` – Configures SNMP version as v2c.
  - `v3` – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels.
    - `auth` – Uses SNMP v3 with authentication and no privacy
    - `noauth` – Uses SNMP v3 with no authentication and no privacy
    - `priv` – Uses SNMP v3 with authentication and privacy

- **notify <WORD>**
  - Optional. Configures the notification view string
    - `<WORD>` – Specify the string (should not exceed 32 characters).

- **read <WORD>**
  - Optional. Configures the read view string
    - `<WORD>` – Specify the string (should not exceed 32 characters).

- **write <WORD>**
  - Optional. Configures the write view string
    - `<WORD>` – Specify the string (should not exceed 32 characters).

### snmp-server host <IP>

Configures SNMP-server related settings

- **host** – Optional. Configures the host(s) receiving the SNMP notifications. At least one SNMP server host should be configured in order to configure the switch to send notifications
  - `<IP>` – Specify the SNMP host’s IP address.

**Note:** You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy.

**Note:** Ensure that SNMP trap notification is enabled.

- **<STRING>**
  - Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the `snmp-server > community <STRING> > {ro|rw}` command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host.
  - `<STRING>` – Specify the community string. The string configured here is sent in the SNMP traps to the SNMPv1 or SNMPv2c hosts.

- **version [v1|v2c|v3 [auth|noauth|priv]]**
  - Configures the SNMP version used
    - `v1` – Configures the SNMP version as 1. This is the default setting.
    - `v2c` – Configures SNMP version as 2c.
    - `v3` – Configures the SNMP version as 3. If using SNMPv3, specify the authentication and encryption levels.
      - `auth` – Uses SNMP v3 with authentication and no privacy
      - `noauth` – Uses SNMP v3 with no authentication and no privacy
      - `priv` – Uses SNMP v3 with authentication and privacy
GLOBAL CONFIGURATION COMMANDS

- **snmp-server {host <IP> inform [retry <0-255>|timeout <0-2147483647>] <STRING> version [v2c|v3 [auth|noauth|priv]]} udp-port <1-65535>}**

  - **snmp-server host <IP>**
    - Configures SNMP-server related settings
    - `host` – Optional. Configures the host(s) receiving the SNMP notifications
    - `<IP>` – Specify the SNMP host’s IP address.
    - **Note:** You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy.
    - **Note:** Ensure that SNMP trap notification is enabled.

  - **inform [retry <0-255>|timeout <0-2147483647>]**
    - Enables sending of SNMP notifications as inform messages, and configures inform message settings.
    - `retry <0-255>` – Configures the maximum number attempts made to re-send an inform message in case the specified SNMP host does not acknowledge receipt.
    - `<0-255>` – Specify a value from 0 - 255. The default is 3.
    - `timeout <0-2147483647>` – Configures the interval, in seconds, to wait for an acknowledgment from the SNMP host before re-sending an inform message.
    - `<0-2147483647>` – Specify a value from 0 - 2147483647 seconds. The default is 1500 seconds.
    - Inform messages are more reliable than trap messages since they include a request for acknowledgement of receipt. Using inform messages to communicate critical information would be good practice. However, since inform messages are retained in the memory until a response is received, they consume more memory and may also result in traffic congestion. Take into considerations these facts when configuring the notification format.

  - **<STRING>**
    - Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the `snmp-server > community <STRING> > {ro|rw} command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host.
    - `<STRING>` – Specify the community string. The string configured here is sent in the SNMP inform messages to the SNMPv2c or SNMPv3 hosts.

  - **version [v2c|v3 [auth|noauth|priv]]**
    - Configures the SNMP version used
    - `v2c` – Configures the SNMP version as v2c
    - `v3` – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels.
      - `auth` – Uses SNMP v3 with authentication and no privacy
      - `noauth` – Uses SNMP v3 with no authentication and no privacy
      - `priv` – Uses SNMP v3 with authentication and privacy
    - **Note:** SNMP inform messages are not supported on SNMP v1.

- **udp-port <1-65535>**
  - Optional. After specifying the SNMP version, optionally specify the host UDP port
  - `<1-65535>` – Specify the UDP port. The default is 162.

- **snmp-server {location <WORD>}}**

  - **snmp-server location <WORD>**
    - Configures SNMP-server related settings
    - `location` – Optional. Configures the EX3500’s location string
    - `<WORD>` – Specify the location (should not exceed 255 characters).
### snmp-server

**snmp-server {notify-filter <WORD> remote <IP>}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notify-filter &lt;WORD&gt;</td>
<td>Optional. Modifies the SNMP server's notify filter name.</td>
</tr>
<tr>
<td>remote &lt;IP&gt;</td>
<td>Optional. Configures the remote host's IP address.</td>
</tr>
</tbody>
</table>

### snmp-server user

**snmp-server user <USER-NAME> <GROUP-NAME> remote <IP> v3 {auth|encrypted auth} [md5|sha] <WORD> {priv [3des|aes128|aes192|aes256|des56] <WORD>}}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user &lt;USER-NAME&gt;</td>
<td>Optional. Configures the name of the SNMP user (connecting to the SNMP agent) and adds the user to an existing SNMP group. It also specifies the SNMP version type used. In case of SNMP version 3, this command also configures the remote host's IP address and the authentication type used.</td>
</tr>
<tr>
<td>&lt;GROUP-NAME&gt;</td>
<td>Specify the SNMP group name to which this user is assigned.</td>
</tr>
<tr>
<td>remote &lt;IP&gt; v3</td>
<td>Configures the remote host on which the SNMPv3 engine is running.</td>
</tr>
<tr>
<td>{auth</td>
<td>encrypted auth} [md5</td>
</tr>
<tr>
<td>{priv [3des</td>
<td>aes128</td>
</tr>
</tbody>
</table>

**Note:** This option is available only for SNMPv3 engine. After configuring the remote host, optionally configure the authentication type and the corresponding authentication password used.

### Optional. Configures authentication and encryption settings

- **auth** – Specifies the authentication type used and configures the authentication password
- **encrypted** – Enables encryption. When enabled all communications between the user and the SNMP engine are encrypted. After enabling encryption, specify the authentication type and configure the authentication password.

The following parameters are common to the 'auth' and 'encrypted' keywords:

- **md5** – Uses MD5 to authenticate the user
- **sha** – Uses SHA to authenticate the user

The following parameter is common to the 'md5' and 'sha' keywords:

- **<WORD>** – Specify the authentication password.

**Note:** If the 'encrypted' option is not being used, enter an 8 - 40 characters ASCII password. Whereas, in case of an encrypted password enter a HEX characters password of 32 characters.

### Optional. Uses SNMPv3 with privacy.

Select one of the privacy options: des, aes128, aes192, aes256, des56

- **<WORD>** – Configures the privacy password. If the 'encrypted' option is not being used, enter an 8 - 40 characters long ASCII password. Whereas, the encrypted password should be 32 HEX characters.
snmp-server user
<USER-NAME>
<GROUP-NAME>
[v1|v2c|v3]

Configures SNMP-server related settings
- user – Optional. Configures the name of the SNMP user (connecting to the SNMP agent) and adds the user to an existing SNMP group. It also specifies the SNMP version type used. In case of SNMPv3, this command also configures the authentication type used and the enables encryption.
- <USER-NAME> – Specify the user’s name (should not exceed 32 characters).
- <GROUP-NAME> – Specify the SNMP group name to which this user is assigned.
- [v1|v2c|v3] – After specifying the group name, specify the SNMP version used. The options are SNMP version v1, SNMP version 2c, and SNMP version 3.

If using SNMP version 3, optionally specify the authentication type and the corresponding authentication password used. Please see previous table for SNMPv3 authentication and encryption configuration details.

snmp-server view
<VIEW-NAME>

Configures SNMP-server related settings
- view – Optional. Creates an SNMP view. SNMP views are used to control user access to the MIB.
- <VIEW-NAME> – Provide a name for this SNMP view (should not exceed 32 characters).

<OID-TREE-STRING>
[excluded|included]

Configures the object identifier (OID) of a branch within the MIB tree
- excluded – Specifies an excluded view
- included – Specifies an included view

Examples
nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server enable traps

nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server host 192.168.13.10 snmpertextstring version 1 udp-port 170

nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server host 1.2.3.4 inform retry 2 test version 3 auth udp-port 180

nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server engine-id local 1234567890

nx9500-6C8809(config-ex3500-management-policy-test)#show context ex3500-management-policy test
http secure-server
enable password level 3 7 12345678901020304050607080929291
snmp-server enable traps authentication
snmp-server notify-filter 3 remote 1.2.3.4
snmp-server notify-filter 1 remote 127.0.0.1
snmp-server notify-filter 2 remote 192.168.13.10
snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port 180
snmp-server host 192.168.13.10 snmpertextstring version 1 udp-port 170
snmp-server engine-id local 1234567890
memory falling-threshold 50
memory rising-threshold 95
process-cpu falling-threshold 60
process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#

Related Commands
no
Removes SNMP server related settings or reverts them to default
4.142.2.6 ssh

**ex3500-management-policy config commands**

Configures the SSH server settings used to authenticate Secure Shell (SSH) connection to a EX3500 switch. Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling un-used and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**
```
ssh [authentication-retries <1-5>|server|server-key size <512-1024>|timeout <1-120>]
```

**Parameters**
- `ssh [authentication-retries <1-5]|server|server-key size <512-1024]|timeout <1-120>]`

<table>
<thead>
<tr>
<th>ssh</th>
<th>Enables SSH management access to an EX3500 switch. This option is disabled by default. Use this command to configure SSH access settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-retries &lt;1-5&gt;</td>
<td>Configures the maximum number of retries made to connect to the SSH server resource.</td>
</tr>
<tr>
<td>server</td>
<td>Enables SSH server connection</td>
</tr>
<tr>
<td>server-key size &lt;512-1024&gt;</td>
<td>Configures the SSH server key size</td>
</tr>
<tr>
<td>timeout &lt;1-120&gt;</td>
<td>Configures the SSH server resource inactivity timeout value in seconds. When the specified time is exceeded, the SSH server resource becomes unreachable and must be re-authenticated.</td>
</tr>
</tbody>
</table>

**Examples**
```
nx9500-6C8809(config-ex3500-management-policy-test)#ssh authentication-retries 4
nx9500-6C8809(config-ex3500-management-policy-test)#ssh timeout 90
nx9500-6C8809(config-ex3500-management-policy-test)#ssh server-key size 600
nx9500-6C8809(config-ex3500-management-policy-test)#ssh server
```

**Related Commands**
```
no
```

Disables SSH management access to an EX3500 switch.
### 4.142.2.7 username

**ex3500-management-policy config commands**

Configures a EX3500 switch user settings

The EX3500 switch user details are stored in a local database on the NX9500, NX7500, NX6500, NX4500 or WiNG VM. You can configure multiple users, each having a unique name, access level, and password.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```
username <USER-NAME> [access-level <0-15>|nopassword|password [0|7] <PASSWORD>]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username &lt;USER-NAME&gt;</td>
<td>Configures the TACACS server port username</td>
</tr>
<tr>
<td>access-level &lt;0-15&gt;</td>
<td>Configures the access level for this user. This value determines the access priority of each user requesting access and interoperability with EX3500 switch.</td>
</tr>
<tr>
<td>nopassword</td>
<td>Allows user to login without a password</td>
</tr>
<tr>
<td>password [0</td>
<td>7] &lt;PASSWORD&gt;</td>
</tr>
<tr>
<td></td>
<td>0 — Configures a plain text password</td>
</tr>
<tr>
<td></td>
<td>7 — Configures an encrypted password (should be 32 characters in length)</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-ex3500-management-policy-test)#username user1 access-level 5

nx9500-6C8809(config-ex3500-management-policy-test)#username user1 password 0 user1@1234

nx9500-nx9500-6C8809(config-ex3500-management-policy-test)#show context

ex3500-management-policy test

ssh server
ssh authentication-retries 4
ssh timeout 90
ssh server-key size 600
http secure-server

enable password level 3 7 1234567890120304050607080929291

username user1 access-level 5
username user1 password 7 5c4786c1e52f913d38168ce89154a079
snmp-server enable traps authentication
snmp-server notify-filter 3 remote 1.2.3.4
snmp-server notify-filter 1 remote 127.0.0.1
```

**Related Commands**

`no` Removes this SNMP user settings
4.1.42.2.8 **no**

**Ex3500-management-policy config commands**

Removes or reverts this EX3500 management policy settings

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```plaintext
no [enable|http|memory|process-cpu|snmp-server|ssh|username]
no enable password {level <0-15>}
no http [port|secure-port|secure-sever|server]
no memory [falling-threshold|rising-threshold]
no process-cpu [falling-threshold|rising-threshold]
no snmp-server {community|contact|enable|engine-id|group|host|location|notify-filter|
  user|view}
no snmp-server {community <STRING>}
no snmp-server {contact}
no snmp-server {enable traps {authentication|link-up-down}}
no snmp-server {engine-id [local|remote <IP>]}
no snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]]}
no snmp-server {host <IP>}
no snmp-server {location}
no snmp-server {notify-filter <WORD> remote <IP>}
no snmp-server {user <USER-NAME> [v1|v2c|v3]}
no snmp-server {user <USER-NAME> <GROUP-NAME> remote-host <IP> v3}
no snmp-server {view <VIEW-NAME> {<OID-TREE-STRING>}}
no ssh [authentication-retries|server|server-key size <512-1024>|timeout]
no username
```

**Parameters**

- no `<PARAMETERS>`

| no `<PARAMETERS>` | Removes this EX3500 management policy settings based on the parameters passed |
Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
ssh server
ssh authentication-retries 4
ssh timeout 90
ssh server-key size 600

http secure-server
enable password level 3 7 12345678901020304050607080929291
username user1 password 7 5c4786c1e52f913d38168ce89154a079
snmp-server enable traps authentication
snmp-server notify-filter 3 remote 1.2.3.4
snmp-server notify-filter 1 remote 127.0.0.1
snmp-server notify-filter 2 remote 192.168.13.10
snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port 180
snmp-server host 192.168.13.10 snmpteststring version 1 udp-port 170
snmp-server engine-id local 1234567890

memory falling-threshold 50
memory rising-threshold 95
process-cpu falling-threshold 60
process-cpu rising-threshold 80

nx9500-6C8809(config-ex3500-management-policy-test)#
```

```
nx9500-6C8809(config-ex3500-management-policy-test)#no http secure-server

nx9500-6C8809(config-ex3500-management-policy-test)#no memory falling-threshold

nx9500-6C8809(config-ex3500-management-policy-test)#no process-cpu rising-threshold

nx9500-6C8809(config-ex3500-management-policy-test)#no snmp-server notify-filter 3 remote 1.2.3.4

nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
ssh server
ssh authentication-retries 4
ssh timeout 90
ssh server-key size 600
enable password level 3 7 12345678901020304050607080929291
username user1 password 7 5c4786c1e52f913d38168ce89154a079
snmp-server enable traps authentication
snmp-server notify-filter 1 remote 127.0.0.1
snmp-server notify-filter 2 remote 192.168.13.10
snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port 180
snmp-server host 192.168.13.10 snmpteststring version 1 udp-port 170
snmp-server engine-id local 1234567890

memory falling-threshold 60

nx9500-6C8809(config-ex3500-management-policy-test)#
```
### 4.1.43 ex3500-qos-class-map-policy

#### Global Configuration Commands

The following table lists EX3500 QoS class map policy configuration mode commands:

**Table 4.22  EX3500-QoS-Class-Map Config Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex3500-qos-class-map-policy</td>
<td>Creates an EX3500 QoS class map policy and enters its configuration mode</td>
<td>page 4-193</td>
</tr>
<tr>
<td>ex3500-qos-class-map-policy config commands</td>
<td>Summarizes EX3500 QoS class map policy configuration mode commands</td>
<td>page 4-194</td>
</tr>
<tr>
<td>ex3500-qos-policy-map</td>
<td>Creates an EX3500 QoS policy map and enters its configuration mode</td>
<td>page 4-200</td>
</tr>
<tr>
<td>ex3500</td>
<td>Creates an EX3500 time range list and enters its configuration mode</td>
<td>page 4-167</td>
</tr>
<tr>
<td>ex3500-management-policy</td>
<td>Creates an EX3500 management policy and enters its configuration mode</td>
<td>page 4-174</td>
</tr>
<tr>
<td>ex3524</td>
<td>Adds a EX3524 switch to the network</td>
<td>page 4-214</td>
</tr>
<tr>
<td>ex3548</td>
<td>Adds a EX3548 switch to the network</td>
<td>page 4-216</td>
</tr>
</tbody>
</table>
4.1.43.1  ex3500-qos-class-map-policy

`ex3500-qos-class-map-policy`

Creates a EX3500 Quality of Service (QoS) class map policy and enters its configuration mode.

A QoS class map policy contains a set of Differentiated Services (DiffServ) classification criteria that are used to classify incoming traffic into different category and provide differentiated service based on this classification. Each policy defines a set match criteria rules that use objects, such as access lists, IP precedence or DSCP values, and VLANs. When configured and applied, the policy classifies traffic based on layer 2, layer 3, or layer 4 information contained in each incoming packet.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax
`ex3500-qos-class-map-policy <POLICY-NAME>`

Parameters
- `ex3500-qos-class-map-policy <POLICY-NAME>`

Examples
```
nx9500-6C8809(config)#ex3500-qos-class-map-policy dscp
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#?
```

```
EX3500_Qos_class_map Mode commands:
  description       Class-map description
  match             Defines the match criteria to classify traffic
  no                Negate a command or set its defaults
  rename            Redefines the name of class-map
  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                 Run commands from Exec mode
  end                End current mode and change to EXEC mode
  exit               End current mode and down to previous mode
  help               Description of the interactive help system
  revert             Revert changes
  service            Service Commands
  show               Show running system information
  write              Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

Related Commands
- `no` Removes an existing EX3500 QoS class map policy
4.1.43.2 ex3500-qos-class-map-policy config commands

The following table summarizes EX3500 QoS class map policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Configures a description for this EX3500 QoS class map policy</td>
<td>page 4-195</td>
</tr>
<tr>
<td>match</td>
<td>Configures match criteria rules used to classify traffic</td>
<td>page 4-196</td>
</tr>
<tr>
<td>rename</td>
<td>Renames an existing EX3500 QoS class map object</td>
<td>page 4-198</td>
</tr>
<tr>
<td>no</td>
<td>Removes this EX3500 QoS class map policy’s description and match criteria</td>
<td>page 4-199</td>
</tr>
</tbody>
</table>
4.1.43.2.1 description

• ex3500-qos-class-map-policy config commands

Configures this EX3500 QoS class map policy’s description

Supported in the following platforms:
• Wireless Controller — RFS7000
• Service Platforms — NX7500, NX9500

Syntax
description <LINE>

Parameters
• description <LINE>

<table>
<thead>
<tr>
<th>description &lt;LINE&gt;</th>
<th>Configures this EX3500 QoS class map policy’s description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;LINE&gt; — Enter a description that allows you to differentiate it from other policies with similar configuration (should not exceed 64 characters)</td>
<td></td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#description "Matches packets marked for DSCP service 3"
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context ex3500-qos-class-map-policy dscp
description "Matches packets marked for DSCP service 3"
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#

Related Commands

• no

| no | Removes this EX3500 QoS class map policy’s description |
4.1.43.2.2 match

**ex3500-qos-class-map-policy config commands**

Configures match criteria rules used to classify traffic.

Access lists, IP precedence, DSCP values, or VLANs are commonly used to classify traffic. Access lists select traffic based on layer 2, layer 3, or layer 4 information contained in each packet.

**Supported in the following platforms:**
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```
```

**Parameters**


  Configures the match criteria. The options are: access-list, cos, ip, ipv6, vlan

  **Note:** Incoming packets matching the specified criteria are included in this QoS class map.

  | access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl] <ACL-NAME> | Uses access lists to provide the match criteria. You can use any one the following ACL types to classify traffic:
  | cos <0-7> | Configures the class of service (CoS) value used to apply user priority. CoS is a form of QoS applicable only to layer 2 Ethernet frames. It uses 3-bits (8 values) of the 802.1Q tag to differentiate and shape network traffic.
  | ip [dscp <0-63]|precedence <0-7>] | Configures the IPv4 DSCP value to match and/or the IP precedence value to match.

Contd...
Usage Guidelines
When configuring match entries, take into consideration the following points:

- Deny rules included in an ACL (associated with a EX3500 QoS class map policy) are ignored whenever an incoming packet matches the ACL.
- A class map policy cannot include both IP ACL or IP precedence rule and a VLAN rule.
- A class map policy containing a MAC ACL or VLAN rule cannot include either an IP ACL or a IP precedence rule.
- A class map policy can include a maximum of 16 match entries.

Examples
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#match ip dscp 3

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context ex3500-qos-class-map-policy dscp
description "Matches packets marked for DSCP service 3"
match ip dscp 3

nx9500-6C8809(config-ex3500-qos-class-map-policy-test2)#match ip precedence 1

Related Commands

- no [Removes match criteria rules configured for this EX3500 QoS class map policy]
4.1.43.2.3 rename

-renamed-list-commands

Renames an existing EX3500 QoS class map policy

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax
rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME>

Parameters

- rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME>

<table>
<thead>
<tr>
<th>rename &lt;EX3500-QOS-CLASS-MAP-POLICY-NAME&gt; &lt;NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME&gt;</th>
<th>Renames an existing EX3500 QoS class map policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;EX3500-QOS-CLASS-MAP-POLICY-NAME&gt;</td>
<td>Enter the EX3500 QoS class map's current name.</td>
</tr>
<tr>
<td>• &lt;NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME&gt;</td>
<td>Enter the new name.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename [TAB]
dscp test test2
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename test2 IP_Precedence

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename [TAB]
dscp IP_Precedence test
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
4.1.43.2.4  no

> ex3500-qos-class-map-policy config commands

Removes this EX3500 QoS class map policy’s description and match criteria

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

no [description|match]

no description

no match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl] <ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-4094>]

Parameters
- no <PARAMETERS>

| no <PARAMETERS> | Removes the EX3500 QoS class map policy’s settings based on the parameters passed |

Examples

The following example shows the EX3500 QoS class map policy ‘test’ settings before the ‘no’ command are executed:

```plaintext
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context ex3500-qos-class-map-policy dscp
description "Matches packets marked for DSCP service 3"
mismatch ip dscp 3
```

```plaintext
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#no description
```

The following example shows the EX3500 QoS class map policy ‘test’ settings after the ‘no’ command are executed:

```plaintext
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context ex3500-qos-class-map-policy test
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```
4.1.44 **ex3500-qos-policy-map**

*Global Configuration Commands*

The following table lists EX3500 QoS policy map configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ex3500-qos-policy-map</code></td>
<td>Creates a EX3500 policy map and enters its configuration mode</td>
<td>page 4-201</td>
</tr>
<tr>
<td><code>ex3500-qos-policy-map config commands</code></td>
<td>Summarizes EX3500 QoS policy map configuration mode commands</td>
<td>page 4-202</td>
</tr>
</tbody>
</table>
4.1.44.1  **ex3500-qos-policy-map**

> **ex3500-qos-policy-map**

Creates an EX3500 policy map and enters its configuration mode

An EX3500 policy map contains one or more EX3500 QoS class maps traffic classifications (existing and configured) and can be attached to multiple interfaces. Creates an EX3500 policy map, and then use the class parameter to configure policies for traffic that matches the criteria defined in the EX3500 QoS class map policy. For more information see, **match**.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```
ex3500-qos-policy-map <EX3500-QOS-POLICY-MAP-NAME>
```

**Parameters**

- **ex3500-qos-policy-map <EX3500-QOS-POLICY-MAP-NAME>**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;EX3500-QOS-POLICY-MAP-NAME&gt;</code></td>
<td>Specify the EX3500 policy map's name</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config)#ex3500-qos-policy-map testPolicyMap
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#?

EX3500_Qos_policy_map Mode commands:

  class       Defines a traffic classification for the policy
  description Policy-map description
  no          Negate a command or set its defaults
  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#
```

**Related Commands**

- **no**  Removes an existing EX3500 QoS policy map
## ex3500-qos-policy-map config commands

The following table summarizes EX3500 QoS policy map configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Creates a policy map class and enters its configuration mode</td>
<td>page 4-203</td>
</tr>
<tr>
<td>description</td>
<td>Configures this EX3500 QoS policy map's description</td>
<td>page 4-212</td>
</tr>
<tr>
<td>no</td>
<td>Removes this EX3500 QoS policy map's settings. Use this keyword to remove or modify the description and to remove the QoS traffic classification created.</td>
<td>page 4-213</td>
</tr>
</tbody>
</table>
### 4.1.44.2.1 `class`

- **ex3500-qos-policy-map config commands**

Creates a policy map class and enters its configuration mode. The policy map class is a traffic classification upon which a policy can act.

**Supported in the following platforms:**
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```
class <EX3500-QoS-CLASS-MAP-POLICY-NAME>
```

**Parameters**

- `class <EX3500-QoS-CLASS-MAP-POLICY-NAME>`

**Examples**

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#class dscp
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#?
commands:
  no       Negate a command or set its defaults
  police   Defines a policer for classified traffic
  set      Classify IP traffic
  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>no</th>
<th>Removes this policy map class association</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ex3500-qos-policy-map</strong></td>
<td>EX3500 QoS policy map configuration mode commands</td>
</tr>
</tbody>
</table>
4.1.44.2.2 ex3500-qos-policy-map-class-config commands

The following table summarizes the policy map class configuration mode commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>police</td>
<td>Configures an enforcer for classified traffic</td>
<td>page 4-205</td>
</tr>
<tr>
<td>set</td>
<td>Sets class of service (CoS) value, per-hop behavior (PHB) value, and IP DSCP value in matching packets</td>
<td>page 4-209</td>
</tr>
<tr>
<td>no</td>
<td>Removes this traffic classification’s settings</td>
<td>page 4-211</td>
</tr>
</tbody>
</table>
4.1.44.2.3  police

Configures an enforcer for classified traffic

Supported in the following platforms:

- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

police [flow|srtcm-color-aware|srtcm-color-blind|trtcm-color-aware|trtcm-color-blind]

police flow <0-1000000> <0-16000000> conform-action transmit violate-action
[<0-63>|drop]

police [srtcm-color-aware|srtcm-color-blind] <0-1000000> <0-16000000> <0-16000000>
conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]

police [trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000>
<0-16000000> conform-action transmit exceed-action [<0-63>|drop]
violate-action [<0-63>|drop]

Parameters

- police flow <0-1000000> <0-16000000> conform-action transmit violate-action
[<0-63>|drop]

<table>
<thead>
<tr>
<th>police</th>
<th>Configures an enforcer for classified traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow &lt;0-1000000&gt; &lt;0-16000000&gt;</td>
<td>Configures an enforcer for classified traffic based on the metered flow rate</td>
</tr>
<tr>
<td>• &lt;0-1000000&gt; – Configures the committed information rate (CIR) from 0 -1000000 kilobits per second.</td>
<td></td>
</tr>
<tr>
<td>• &lt;0-16000000&gt; – Configures the committed burst size (BC) from 0 - 16000000 bytes.</td>
<td></td>
</tr>
<tr>
<td>Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is specified by the committed-burst field, and the average rate tokens are added to the bucket is specified by the committed-rate option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.</td>
<td></td>
</tr>
<tr>
<td>The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented CIR and the maximum size of the token bucket BC.</td>
<td></td>
</tr>
<tr>
<td>The token bucket C is initially full, that is, the token count Tc(0) = BC. Thereafter, the token count Tc is updated CIR times per second as follows:</td>
<td></td>
</tr>
<tr>
<td>• If Tc is less than BC, Tc is incremented by one, else</td>
<td></td>
</tr>
<tr>
<td>• Tc is not incremented.</td>
<td></td>
</tr>
<tr>
<td>When a packet of size B bytes arrives at time t, the following happens:</td>
<td></td>
</tr>
<tr>
<td>• If Tc(t)-B &gt; OR = 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else</td>
<td></td>
</tr>
<tr>
<td>• The packet is red and Tc is not decremented.</td>
<td></td>
</tr>
<tr>
<td>conform-action transmit</td>
<td>Configures the action applied when packets fall within the specified CIR and BC limits</td>
</tr>
<tr>
<td>• transmit – Transmits packets falling within the specified CIR and BC limits. This is subject to there being enough tokens to service the packet, in which case the packet is set green.</td>
<td></td>
</tr>
<tr>
<td>violate-action [&lt;0-63&gt;</td>
<td>drop]</td>
</tr>
<tr>
<td>• &lt;0-63&gt; – Applies a new DSCP value. Select the DSCP value from 0 -63.</td>
<td></td>
</tr>
<tr>
<td>• drops – Drops packets violating the specified CIR and BC limits</td>
<td></td>
</tr>
</tbody>
</table>
police [srtcm-color-aware|srtcm-color-blind] <0-1000000> <0-16000000> <0-16000000>
conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]

<table>
<thead>
<tr>
<th>police</th>
<th>Configures an enforcer for classified traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[srtcm-color-aware</td>
<td>srtcm-color-blind] &lt;0-1000000&gt; &lt;0-16000000&gt; &lt;0-16000000&gt;</td>
</tr>
<tr>
<td>conform-action transmit</td>
<td>Configures the action applied when packet rates fall within the specified CIR and BC limits</td>
</tr>
<tr>
<td>transmit</td>
<td>transmit – Transmits packets falling within the specified CIR and BC limits</td>
</tr>
</tbody>
</table>
police Configures an enforcer for classified traffic
[trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000> <0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]

exceed-action
[<0-63>|drop]
Configures the action applied when packet rates exceed the specified CIR and BC limits
• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 -63.
• drops – Drops packets exceeding the specified CIR and BC limits

violate-action
[<0-63>|drop]
Configures the action applied when packet rates exceed the specified BE limit
• <0-63> – Applies a new DSCP value. Select the DSCP value from 0 -63.
• drops – Drops packets exceeding the specified BE limit

• police [trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000> <0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]

police Configures an enforcer for classified traffic
[trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000> <0-16000000>
• trtcm-color-blind - Two rate three color meter in color-blind mode
• trtcm-color-aware - Two rate three color meter in color-aware mode
  • <0-1000000> – Configures the CIR from 0 - 1000000 kilobits per second
  • <0-16000000> – Configures the BC from 0 - 16000000 bytes.
  • <0-1000000> – Configures the PIR from 0 - 1000000 kilobits per second
  • <0-16000000> – Configures the BP from 0 - 16000000 bytes

The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.

The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:
• If Tp(t)-B < 0, the packet is red, else
• if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
• The packet is green and both Tp and Tc are decremented by B.

Contd..
### Usage Guidelines

When configuring the traffic class enforcer parameters, take into consideration the following factors:

1. You can configure up to 200 enforcers/policers (i.e., class maps) for ingress ports.
2. The committed-rate cannot exceed the configured interface speed, and the committed-burst cannot exceed 16 Mbytes.

### Examples

The following example uses the police trtcn-color-blind command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 Kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)
police trtcn-color-blind 100000 4000 100000 6000 conform-action transmit exceed-action 0 violate-action drop
```

### Related Commands

- **no**
  - Removes the traffic enforcer settings
4.1.44.2.4  set

Sets class of service (CoS) value, per-hop behavior (PHB) value, and IP DSCP value in matching packets.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

```bash
set [cos <0-7>|ip dscp <0-63>|phb <0-7>]
```

Parameters

- **set [cos <0-7>|ip dscp <0-63>|phb <0-7>]**

<table>
<thead>
<tr>
<th>set</th>
<th>Sets the match criteria used to identify and classify traffic into different classes. The match criteria options are: CoS, IP DSCP, and PHB values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cos &lt;0-7&gt;</td>
<td>Configures the CoS value for a matching packet (as specified by the match command) in the packet's VLAN tag. &lt;0-7&gt; — Specify a value from 0 - 7. The CoS is modified to the value specified here.</td>
</tr>
<tr>
<td>ip dscp &lt;0-63&gt;</td>
<td>Modifies the IP DSCP value in a matching packet (as specified by the match command) &lt;0-63&gt; — Specify a value from 0 - 63. The DSCP value is modified to the value specified here.</td>
</tr>
<tr>
<td>phb &lt;0-7&gt;</td>
<td>Configures a PHB value for a matching packets. &lt;0-7&gt; — Specify a value from 0 - 7. <strong>Note:</strong> The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green, yellow, or red as per the following: • green if it does not exceed the CIR and BC limits • yellow if it exceeds the CIR and BC limits, but not the BE limit, and • red otherwise.</td>
</tr>
</tbody>
</table>

Examples

The following example uses the `set > phb` command to classify the service that incoming packets will receive, and then uses the `police > trtcm-color-blind` command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 Kbps, the peak burst size to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```bash
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#set phb 3
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#police trtcm-color-blind 100000 4000 1000000 6000 conform-action transmit exceed-action 0 violate-action drop
```

The following example uses the `set > ip dscp` command to classify the service that incoming packets will receive, and then uses the `police > flow` command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets:

```bash
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#set ip dscp 3
```
```bash
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#police flow 100000 4000 conform-action transmit violate-action drop

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context class dscp
  set ip dscp 3
  police flow 100000 4000 conform-action transmit violate-action drop

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes CoS value, PHB value, or IP DSCP value from this traffic class</td>
</tr>
</tbody>
</table>
4.1.44.2.5  no

ex3500-qos-policy-map-class-config commands

Removes this traffic classification’s settings

Supported in the following platforms:
• Wireless Controller — RFS7000
• Service Platforms — NX7500, NX9500

Syntax
no [police|set]

no police [flow|srtcm-color-aware|srtcm-color-blind|trtcm-color-aware|
  trtcm-color-blind]

no set [cos|ip dscp|phb]

Parameters
• no <PARAMETERS>

no <PARAMETERS> Removes this traffic class settings based on the parameters passed

Examples

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context
  class dscp
    set ip dscp 3
    police flow 100000 4000 conform-action transmit violate-action drop

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no set ip
dscp

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no police
flow

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no police

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context
class dscp

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
### 4.1.44.2.6 description

**ex3500-qos-policy-map config commands**

Configures this EX3500 QoS policy map's description

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

description <LINE>

**Parameters**

- description <LINE>

<table>
<thead>
<tr>
<th>description &lt;LINE&gt;</th>
<th>Configures this EX3500 QoS policy map's description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;LINE&gt; – Enter a description that allows you to differentiate it from other policies with similar configuration (should not exceed 64 characters)</td>
</tr>
</tbody>
</table>

**Examples**

nx9500-6C8809(config-ex3500-qos-policy-map-test)#description "This is a test EX3500 QoS Policy Map"

nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
description "This is a test EX3500 QoS Policy Map"
class test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#

**Related Commands**

- **no** Removes this EX3500 QoS policy map's description
4.1.44.2.7 no

* ex3500-qos-policy-map config commands

Removes this EX3500 QoS policy map's settings. Use this keyword to remove the description and to remove the QoS traffic classification created.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

**Syntax**

```
no [class <EX3500-QoS-POLICY-MAP-NAME>|description]
```

**Parameters**

- no <PARAMETERS>

 **Examples**

The following example shows the EX3500 QoS policy map 'test' settings before the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
description "This is a test EX3500 QoS Policy Map"
class test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
```

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#no description
```

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#no class test
```

The following example shows the EX3500 QoS policy map 'test' settings after the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
```
4.1.45 ex3524

Global Configuration Commands

Adds a EX3524 switch to the network

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four Small Form Factor Pluggable (SFP) transceiver slots for fiber connectivity.

To enable layer 3 adoption of the logged EX3524 switch to a NOC controller, navigate to the EX3524 switch’s device configuration mode and execute the following command: controller > host > <IP/HOSTANME>.

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

Going forward NX9500, NX7500, NX6500, NX4500 WiNG managed series service platforms and WiNG VMs can discover, adopt, and partially manage EX3500 series Ethernet switches without modifying the proprietary operating system running the EX3500 switches. The WiNG service platforms utilize standardized WiNG interfaces to push configuration files to the EX3500 switches, and maintain a translation layer, understood by the EX3500 switch, for statistics retrieval.

Supported in the following platforms:
- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

ex3524 <DEVICE-EX3524-MAC>

Parameters

- ex3524 <DEVICE-EX3524-MAC>

Examples

nx9500-6C8809(config)#ex3524 A1-C4-33-6D-66-07

nx9500-6C8809(config-device-A1-C4-33-6D-66-07)#?

EX35xx Device Mode commands:

- hostname Set system's network name
- interface Select an interface to configure
- ip Internet Protocol (IP)
- no Negate a command or set its defaults
- power EX3500 Power over Ethernet Command
- remove-override Remove configuration item override from the device (so profile value takes effect)
- upgrade Configures upgrade option for ex3500 system
- use Set setting to use
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal
nx9500-6C8809(config-device-A1-C4-33-6D-66-07)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a EX3524 switch from the network</td>
</tr>
</tbody>
</table>
4.1.46 ex3548

Global Configuration Commands

Adds a EX3548 switch to the network

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity.

Supported in the following platforms:

- Wireless Controller — RFS7000
- Service Platforms — NX7500, NX9500

Syntax

```
ex3548 <DEVICE-EX3548-MAC>
```

Parameters

- `ex3548 <DEVICE-EX3548-MAC>`

Examples

```
nx9500-6C8809(config)#ex3548 22-65-78-09-12-35
nx9500-6C8809(config-device-22-65-78-09-12-35)#?
```

<DEVICE-EX3548-MAC> | Specifies the MAC address of a EX3548 switch
--- | ---

EX35xx Device Mode commands:

- `hostname` Set system's network name
- `interface` Select an interface to configure
- `ip` Internet Protocol (IP)
- `no` Negate a command or set its defaults
- `power` EX3500 Power over Ethernet Command
- `remove-override` Remove configuration item override from the device (so profile value takes effect)
- `upgrade` Configures upgrade option for ex3500 system
- `use` Set setting to use
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
nx9500-6C8809(config-device-22-65-78-09-12-35)#
```

Related Commands

- `no` Removes a EX3548 switch from the network
4.1.47 firewall-policy

**Global Configuration Commands**

Configures a firewall policy. This policy defines a set of rules for managing network traffic and prevents unauthorized access to the network behind the firewall.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`firewall-policy <FIREWALL-POLICY-NAME>`

**Parameters**

- `firewall-policy <FIREWALL-POLICY-NAME>`

<table>
<thead>
<tr>
<th>&lt;FIREWALL-POLICY-NAME&gt;</th>
<th>Specify the firewall policy name. If a firewall policy does not exist, it is created.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#?
```

Firewall policy Mode commands:

- `acl-logging` Log on flow creating traffic
- `alg` Enable ALG
- `clamp` Clamp value
- `dhcp-offer-convert` Enable conversion of broadcast dhcp offers to unicast
- `dns-snoop` DNS Snooping
- `firewall` Wireless firewall
- `flow` Firewall flow
- `ip` Internet Protocol (IP)
- `ip-mac` Action based on ip-mac table
- `ipv6` Internet Protocol version 6 (IPv6)
- `ipv6-mac` Action based on ipv6-mac table
- `logging` Firewall enhanced logging
- `no` Negate a command or set its defaults
- `proxy-arp` Enable generation of ARP responses on behalf of another device
- `proxy-nd` Enable generation of ND responses (for IPv6) on behalf of another device
- `stateful-packet-inspection-l2` Enable stateful packet inspection in layer2 firewall
- `storm-control` Storm-control
- `virtual-defragmentation` Enable virtual defragmentation for IPv4 packets (recommended for proper functioning of firewall)

```
rfs7000-37FABE(config-fw-policy-test)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes an existing firewall policy</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on Firewall policy, see Chapter 13, FIREWALL-POLICY.
4.1.48 global-association-list

Configures a global list of client MAC addresses. Based on the deny or permit rules specified, clients are either allowed or denied access to the managed network.

The global association list serves the same purpose as an Association Access Control List (ACL). However, the Association ACL allows a limited number of entries, a few thousand only, and does not suffice the requirements of a large deployment. This gap is filled by a global association list, which is much larger (with tens of thousands of entries). Both lists co-exist in the system. When an access request comes in, the association ACL is looked up first and if the requesting MAC address is listed in one of the deny ACLs, the association is denied. But, if the requesting client is permitted access, or if in case none of the ACLs list the client's MAC address, the global association ACL is checked. Once authenticated, the client's credentials are cached on the access point, and subsequent requests are not referenced to the controller. An entry in an APs credential cache means a pass in the global association list.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

global-association-list <GLOBAL-ASSOC-LIST-NAME>

Parameters

- <GLOBAL-ASSOC-LIST-NAME>

Specify the global association list name. If a list with the same name does not exist, it is created.

**Note:** Map this global association list to a device (controller) or a controller profile. Once associated, the controller applies this association list to requests received from all adopted APs. For more information, see **use**.

**Note:** The global association list can also be mapped to a WLAN. The usage of global access lists is controlled on a per-WLAN basis. For more information, see **association-list**.

Examples

rfs4000-229D58(config)#global-association-list my-clients
rfs4000-229D58(config-global-assoc-list-my-clients)#?

Global Association List Mode commands:

- default-action Configure the default action when the client MAC does not match any rule
- deny Specify MAC addresses to be denied
- no Negate a command or set its defaults
- permit Specify MAC addresses to be permitted
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs4000-229D58(config-global-assoc-list-my-clients)#
rfs4000-229D58 (config-global-assoc-list-my-clients)#permit 00-23-69-11-E6-C4
description "10th floor Lab1 Workstation1"

rfs4000-229D58 (config-global-assoc-list-my-clients)#show context
global-association-list my-clients
  permit 00-23-69-11-E6-C4 description "10th floor Lab1 Workstation1"

rfs4000-229D58 (config)#show context
!
! Configuration of RFS4000 version 5.8.1.0-013D
!
! version 2.3
!
client-identity TestClientIdentity
dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
  client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL

....................
global-association-list my-clients
  permit 00-23-69-11-E6-C4 description "10th floor Lab1 Workstation1"

! global-association-list test
  permit 11-22-33-44-55-66 description test
deny 22-33-44-55-66-77 description "Test Deny"
!
captive-portal test
--More--

rfs4000-229D58 (config)#{

rfs4000-229D58 (config-device-00-23-68-22-9D-58)#use global-assoc-list server my-clients

rfs4000-229D58 (config-device-00-23-68-22-9D-58)#show context
rfs4000 00-23-68-22-9D-58
use profile default-rfs4000
use rf-domain default
hostname rfs4000-229D58
license AP DEFAULT-6AP-LICENSE
license ADSEC DEFAULT-ADV-SEC-LICENSE
ip default-gateway 192.168.13.2
ip default-gateway priority static-route 20
interface ge1
  switchport mode access
  switchport access vlan 1
interface vlan1
  ip address 192.168.13.9/24
  ip address 192.168.0.1/24 secondary
  ip dhcp client request options all
use global-association-list server my-clients
use client-identity-group ClientIdentityGroup
logging on
logging console warnings
logging buffered warnings
rfs4000-229D58 (config-device-00-23-68-22-9D-58)#
4.1.49 guest-management

The following table summarizes the guest management policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest-management</td>
<td>Creates a guest management policy and enters its configuration mode</td>
<td>page 4-222</td>
</tr>
<tr>
<td>guest-management-policy-mode</td>
<td>Summarizes guest management policy configuration mode commands</td>
<td>page 4-223</td>
</tr>
</tbody>
</table>

Table 4.27 Guest-Management Policy Config Command
4.1.49.1 guest-management

Configures a guest management policy that redirects guest users to a registration portal upon association to a captive portal SSID. Guest users are redirected to an internally (or) externally hosted registration page (registration.html) where previously, not-registered guest users can register. The internally hosted captive portal registration page can be customized based on business requirements. For more information, see [webpage](#).

Use the guest management policy commands to configure parameters, such as E-mail host and SMS gateway along with the credentials required for sending pass code to guest via e-mail and SMS. You can configure up to 32 different guest management policies. Each guest management policy allows you to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents, and E-mail message body. Although, at any point-in-time, multiple guest management policies may exist, only one guest management policy can be active per device.

Guest registration is supported only on the NX9000 and NX7500 series service platforms as an adopting controller. But the number of user identity entries supported on each varies. It is 2 million and 1 million user identity entries for the NX9000 and NX7500 model service platforms respectively. Guest management and registration is not supported on any of the other WiNG supported platforms.

Supported in the following platforms:
- Service Platforms — NX7500, NX7510, NX75 20, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

guest-management <POLICY-NAME>

**Parameters**
- guest-management <POLICY-NAME>

**Examples**

```
nx9500-6C8809(config)#guest-management guest
nx9500-6C8809(config-guest-management-guest)#?
```

Guest Management Mode commands:
- email                  Email guest-notification configuration
- guest-database-backup  Configure guest-database-backup parameters
- no                     Negate a command or set its defaults
- sms                    SMS guest-notification configuration
- sms-over-smtp          Sms-over-smtp configuration to email sms gateway address
- clrscr                 Clears the display screen
- commit                 Commit all changes made in this session
- do                     Run commands from Exec mode
- end                    End current mode and change to EXEC mode
- exit                   End current mode and down to previous mode
- help                   Description of the interactive help system
- revert                 Revert changes
- service                Service Commands
- show                   Show running system information
- write                  Write running configuration to memory or terminal

```
nx9500-6C8809(config-guest-management-guest)#
```

**Related Commands**

- no                     Removes an existing guest management policy
4.1.49.2 guest-management-policy-mode commands

The following table summarizes guest management policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>Configures guest user e-mail notification settings</td>
<td>page 4-224</td>
</tr>
<tr>
<td>guest-database-backup</td>
<td>Enables periodic backup of the captive portal’s guest registration user database</td>
<td>page 4-226</td>
</tr>
<tr>
<td>sms</td>
<td>Configures guest user SMS notification settings</td>
<td>page 4-227</td>
</tr>
<tr>
<td>sms-over-smtp</td>
<td>Configures an e-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway e-mail address to which the message is E-mailed. The gateway server converts the e-mail into SMS and sends the message to the guest users’s mobile device</td>
<td>page 4-229</td>
</tr>
<tr>
<td>no</td>
<td>Removes this guest management policy settings</td>
<td>page 4-231</td>
</tr>
</tbody>
</table>
4.1.49.2.1  email

guest-management-policy-mode commands

Configures guest user e-mail notification settings

Guest users can register themselves with their e-mail credentials as a primary key for authentication. The captive portal system provides the pass code for their registration. Guest users need to use their registered e-mail, mobile, or member ID and the received pass code for further login to the captive portal.

Supported in the following platforms:
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
email [host|message|subject]
email host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>
  security [none|ssl|starttls] username <USER-NAME> password <PASSWORD>
email message <LINE>
email subject <LINE>
```

Parameters

- `email host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>`
  - Configures the SMTP server resource’s IPv4 address or hostname used for guest management email traffic, guest user credential validation, and pass code reception. Optionally you can use an existing host alias to identify the SMTP server resource.
  - `<IP/HOSTNAME>` – Specify the SMTP server resource’s IP address or hostname.
  - `<HOST-ALIAS-NAME>` – Specify the host alias name (should be existing and configured). Consider providing the host as an alias. A host alias is a configuration item that maps the alias to a hostname. Once created, it can be used across different configuration modes. Where ever used the alias is replaced by the associated hostname.

- `sender <EMAIL-ADDRESS>`
  - Configures the sender’s e-mail address. The sender here is the guest user receiving the pass code. Guest users require this pass code for registering their guest e-mail credentials.
  - `<EMAIL-SENDER>` – Specify the e-mail address (should not exceed 100 characters).

- `security [none|ssl|starttls] username <USER-NAME> password <PASSWORD>`
  - Configures the encryption protocol used by the SMTP server when communicating the pass code.
  - `none` – No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.
  - `SSL` – Uses SSL encryption. This is the default setting.
  - `STARTTLS` – Uses STARTTLS encryption.

- `username <USER-NAME>`
  - Configures a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. Ensure that the password is correctly provided to receive the pass code required for registering guest user credentials with SMS.
  - `<USER-NAME>` – Specify the username (should not exceed 100 characters).

- `password <PASSWORD>`
  - Configures the password associated with the specified SMTP user name
  - `<PASSWORD>` – Specify the password (should not exceed 63 characters).
### email message <LINE>

<table>
<thead>
<tr>
<th>email</th>
<th>Configures guest user e-mail notification content</th>
</tr>
</thead>
<tbody>
<tr>
<td>message &lt;LINE&gt;</td>
<td>Configures the content of the e-mail sent to the guest user notifying the pass code (should not exceed 1024 characters)</td>
</tr>
<tr>
<td></td>
<td>- &lt;LINE&gt; – Specify the message content. When entering the message, use the following tags:</td>
</tr>
<tr>
<td></td>
<td>GM-NAME – for the guest user’s name</td>
</tr>
<tr>
<td></td>
<td>GM_PASSCODE – for the pass code</td>
</tr>
<tr>
<td></td>
<td>CR-NL – to enter a new line</td>
</tr>
<tr>
<td></td>
<td>For example: Dear GM_NAME, CR-NL your internet access pass code is GM_PASSCODE. CR-NL Use this for internet access.</td>
</tr>
</tbody>
</table>

### email subject <LINE>

<table>
<thead>
<tr>
<th>email</th>
<th>Configures guest user e-mail notification subject line</th>
</tr>
</thead>
<tbody>
<tr>
<td>subject &lt;LINE&gt;</td>
<td>Configures the subject line of the e-mail sent to the guest user notifying the pass code (should not exceed 100 characters)</td>
</tr>
<tr>
<td></td>
<td>- &lt;LINE&gt; – Specify the subject line content. When entering the subject line, use the following tag:</td>
</tr>
<tr>
<td></td>
<td>GM-NAME – for the guest user’s name</td>
</tr>
<tr>
<td></td>
<td>For example: GM_NAME, your internet access code</td>
</tr>
</tbody>
</table>

**Examples**

```text
nx9500-6C8809(config-guest-management-test)#email host 192.168.13.10 sender bob@zebra.com security ssl username guest1 password guest1@123

nx9500-6C8809(config-guest-management-test)#show context
guest-management test
  email host 192.168.13.10 sender bob@zebra.com security ssl username guest1 password guest1@123

nx9500-6C8809(config-guest-management-test2)#

nx9500-6C8809(config-guest-management-test2)#email message Dear GM_Guest2, CR-NL Your internet access passcode is GM_Guest2. CR-NL Use this for internet access.

nx9500-6C8809(config-guest-management-test2)#email subject GM_Guest2 Your internet access passcode

nx9500-6C8809(config-guest-management-test2)#show context
guest-management test2
  email subject GM_Guest2 Your internet access passcode
  email message Dear GM_Guest2, CR-NL Your internet access passcode is GM_Guest2. CR-NL Use this for internet access.
```

**Related Commands**

| no                      | Removes the e-mail settings used to send notification mails to the guest user |
4.1.49.2.2 guest-database-backup

Enables periodic backup of a captive portal’s guest registration user database. This option is enabled by default. Supported in the following platforms:

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
guest-database-backup enable {<TIME>}
```

**Parameters**

- `guest-database-backup enable {<TIME>}`

| guest-database-backup enable <TIME> | Enables periodic backup of a captive portal’s guest registration user database. This command also allows you to configure the time at which the system starts backing up the database. The default backup-start time is ‘00:00’ (midnight every day).
|-------------------------------------|----------------------------------------------------------------------------------------
| - `<TIME>` – Optional. Resets the periodic database backup-start time to a user-defined value in the HH;MM format. When specified, the system starts periodic backup of the database, every day, at the specified time. |

**Examples**

nx9500-6C8809(config-guest-management-test)#guest-database-backup enable 12:30

vx9500-6C8809(config-guest-management-test)#show context
guest-management test
guest-database-backup enable 12:30

nx9500-6C8809(config-guest-management-test)#

**Related Commands**

- `no` Disables periodic backup of a captive portal’s guest registration user database
### 4.1.49.2.3 sms

**guest-management-policy-mode commands**

Configures guest user SMS notification settings

SMS enables guest users to register themselves with their e-mail or mobile device ID as the primary key for authentication. The captive portal provides the pass code for registration. Guest users use their registered e-mail or mobile device ID and the received pass code for future login to the captive portal.

![Checkmark](image)

**NOTE:** When using SMS, ensure that the WLAN’s mode of authentication is set to *none* and the mode of registration is set to *user*. In other words, captive portal authentication must always enforce guest registration.

SMS is similar to MAC address-based self registration, but in addition the captive portal sends an SMS message, containing an access code, to the user’s mobile phone number provided at the time of registration. The captive portal verifies the code, returns the *Welcome* page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

The default gateway used with SMS is *Clickatell*. A pass code can be sent with SMS to the guest user directly using Clickatell, or the pass code can be sent via e-mail to the SMS Clickatell gateway server, and Clickatell sends the pass code SMS to the guest user.

Supported in the following platforms:

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
sms [host|message]
```

```
sms host clickatell username <USER-NAME> password <PASSWORD> api-id <ID> user-agent <PYCLICKATELL> {source-number <WORD>}
```

```
sms message <LINE>
```

**Parameters**

- `sms host clickatell username <USER-NAME> password <PASSWORD> api-id <ID> user-agent <PYCLICKATELL> {source-number <WORD>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sms</td>
<td>Configures guest user SMS notification settings</td>
</tr>
<tr>
<td>host clickatell</td>
<td>By default, <em>clickatell</em> is the host SMS gateway server resource. Upon receiving the pass code e-mail, the SMS gateway sends the actual notification pass code SMS to the guest user.</td>
</tr>
<tr>
<td>username &lt;USER-NAME&gt;</td>
<td>Configures a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. Ensure that the password is correctly provided to receive the pass code required for registering guest user credentials with SMS.</td>
</tr>
<tr>
<td>password &lt;PASSWORD&gt;</td>
<td>Configures the password associated with the specified username</td>
</tr>
<tr>
<td>api-id &lt;ID&gt;</td>
<td>Set a 32 character maximum API ID</td>
</tr>
<tr>
<td>user-agent &lt;PYCLICKATELL&gt;</td>
<td>Since the SMS service provider by default is Clickatell, set the user agent name to <em>pyclickatell</em>. The user-agent value ensures the Clickatell SMS gateway server and its related credentials, needed for sending the pass code to guest users, are configured.</td>
</tr>
</tbody>
</table>
### Example

```bash
nx9500-6C8809(config-guest-management-test)#sms host clickatell username guest1 password guest1@123 api-id test user-agent pyclickatell
```

```bash
nx9500-6C8809(config-guest-management-test)#sms message Dear guest1, Your passcode for internet access is GM-guest1
```

```bash
nx9500-6C8809(config-guest-management-test)#show context
guest-management test
  email host 192.168.13.10 sender bob@zebra.com security ssl username guest1 password guest1@123
  sms host clickatell username guest1 password guest1@123 api-id test user-agent pyclickatell
  sms message Dear guest1, Your passcode for internet access is GM-guest1
```

### Related Commands

- `no` - Removes the SMS settings used to send SMS to the guest user
4.1.49.2.4  sms-over-smtp

Configures an e-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway e-mail address to which the message is E-mailed. The gateway server converts the e-mail into SMS and sends the message to the guest users's mobile device.

When sending an e-mail, the e-mail client interacts with a SMTP server to handle the content transmission. The SMTP server on the host may have conversations with other SMTP servers to deliver the e-mail.

Supported in the following platforms:
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```text
sms-over-smtp [host|message|subject]
```

```text
sms-over-smtp  host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>
security [none|ssl|starttls] username <USER-NAME> password <PASSWORD> recipient <EMAIL-ADDRESS>
```

```text
sms-over-smtp  message <LINE>
```

```text
sms-over-smtp  subject <LINE>
```

Parameters

- **sms-over-smtp host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>]**
  - `host` - Configures the SMS gateway server resource’s IPv4 address or hostname used for guest management SMS over SMTP traffic, guest user credential validation and pass code reception. Optionally you can use an existing host alias to identify the SMS gateway server resource.
    - <IP/HOSTNAME> – Specify the SMTP gateway server resource’s IP address or hostname.
    - <HOST-ALIAS-NAME> – Specify the host alias name (should existing and configured). Consider providing the host as an alias. A host alias is a configuration item that maps the alias to a hostname. Once created, it can be used across different configuration modes. Where ever used the alias is replaced by the associated hostname.

- **sms-over-smtp sender <EMAIL-ADDRESS>**
  - `sender` - Configures the sender’s e-mail address. The sender here is the guest user receiving the pass code. Guest users require this pass code for registering their guest e-mail credentials using SMTP.
    - <EMAIL-ADDRESS> – Specify the e-mail address (should not exceed 64 characters).

- **sms-over-smtp security [none|ssl|starttls]**
  - `security` - Configures the encryption protocol used by the SMTP server when communicating the pass code
    - none – No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.
    - SSL – Uses SSL encryption. This is the default setting.
    - STARTTLS – Uses STARTTLS encryption

- **sms-over-smtp username <USER-NAME> password <PASSWORD> recipient <EMAIL-ADDRESS>**
  - `username` - Specifies the username for the SMTP server.
  - `password` - Specifies the password for the SMTP server.
  - `recipient` - Specifies the recipient e-mail address.
username <USER-NAME>  Configures a username unique to this SMTP guest management configuration. After configuring the username, specify the associated password. Ensure that the correct password is provided to receive the pass code required for registering guest user credentials with SMTP.
  • <USER-NAME> – Specify the username (should not exceed 64 characters).

password <PASSWORD>  Configures the password associated with the specified SMTP user name
  • <PASSWORD> – Specify the password (should not exceed 64 characters).

recipient <EMAIL-ADDRESS>  Configures the e-mail recipient's e-mail address
  • <EMAIL-ADDRESS> – Specify the recipient's e-mail address (should not exceed 64 characters in length).

• sms-over-smtp message <LINE>

sms-over-smtp  Configures guest user SMS over SMTP notification message content

message <LINE>  Configures the content of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 1024 characters)
  • <LINE> – Specify the message content. When entering the message, use the following tags:
    GM-NAME – for the guest user's name
    GM_PASSCODE – for the pass code
    CR-NL – to enter a new line
    For example: Dear GM_NAME, CR-NL your internet access pass code is GM_PASSCODE. CR-NL Use this access code for internet access.

• sms-over-smtp subject <LINE>

sms-over-smtp  Configures guest user e-mail notification subject line content

subject <LINE>  Configures the subject line of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 100 characters)
  • <LINE> – Specify the subject line content. When entering the subject line, use the following tag:
    GM-NAME – for the guest user's name
    For example: GM_NAME, your internet access code

Examples

nx9500-6C8809(config-guest-management-test3)#sms-over-smtp host test sender bob@zebra.com security ssl username bob password bob@123 recipient bob@zebra.com

nx9500-6C8809(config-guest-management-test3)#show context guest-management test3
  sms-over-smtp host test sender bob@zebra.com security ssl username bob password bob@123 recipient bob@zebra.com

nx9500-6C8809(config-guest-management-test3)#

Related Commands

no  Removes the SMS over SMTP settings used to send SMS to the guest user
4.1.49.25 no

\textit{guest-management-policy-mode commands}

Removes this guest management policy settings

Supported in the following platforms:
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no \{email|guest-database-backup|sms|sms-over-smtp\}
no email \{host|message|subject\}
no guest-database-backup enable
no sms \{host|message\}
no sms-over-smtp \{host|message|subject\}

Parameters
- no <PARAMETERS>

\begin{tabular}{|l|}
\hline
no <PARAMETERS> & Removes this guest management policy settings based on the parameters passed \\
\hline
\end{tabular}

Examples

nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
  sms-over-smtp host test sender bob@zebra.com security ssl username bob password bob@123
  recipient bob@zebra.com
nx9500-6C8809(config-guest-management-test3)#

nx9500-6C8809(config-guest-management-test3)#no sms-over-smtp host

nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
nx9500-6C8809(config-guest-management-test3)#
4.1.50 **host**

- **Global Configuration Commands**

Enters the configuration context of a remote device using its hostname

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
host <DEVICE-NAME>
```

**Parameters**

- host <DEVICE-NAME>

  **<DEVICE-NAME>**

  Specify the device's hostname. All discovered devices are displayed when 'Tab' is pressed to auto complete this command.

**Examples**

```
rfs4000-229D58(config)#host rfs4000-229D58
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```
4.1.51 inline-password-encryption

Stores the encryption key in the startup configuration file

By default, the encryption key is not stored in the startup-config file. Use the inline-password-encryption command to move the encrypted key to the startup-config file. This command uses the master key to encrypt the password, then moves it to the startup-config file.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
inline-password-encryption

Parameters
None

Usage Guidelines
When the configuration file is imported to a different device, it first decrypts the encryption key using the default key and then decrypts the rest of the configuration using the administrator configured encryption key.

Examples
rfs7000-37FABE(config)#password-encryption secret 2 12345678
rfs7000-37FABE(config)#commit write memory

This command uses the specified password for encryption key and stores it outside of startup-config.

rfs7000-37FABE(config)#inline-password-encryption
This command moves the same password to the startup-config and encrypts it with the master key.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables storing of the encryption key in the startup configuration file</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Enables password encryption</td>
</tr>
</tbody>
</table>
4.1.52 ip

Global Configuration Commands

Creates a IP access control list (ACL) and/or a SNMP IP ACL.

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ip [access-list|snmp-access-list]

ip access-list <IP-ACL-NAME>
ip snmp-access-list <IP-SNMP-ACL-NAME>

Parameters

- **ip access-list <IP-ACL-NAME>**
  - Access-list
  - <IP-ACL-NAME>
    - Creates an IP ACL and enters its configuration mode
    - <IP-ACL-NAME> — Specify the ACL name. If the access list does not exist, it is created.

- **ip snmp-access-list <IP-SNMP-ACL-NAME>**
  - Snmp-access-list
  - <IP-SNMP-ACL-NAME>
    - Creates a SNMP IP ACL and enters its configuration mode. An SNMP IP ACL is an access control mechanism that uses a combination of IP ACL and SNMP community string.
    - SNMP performs network management functions using a data structure called a Management Information Base (MIB). SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.
    - Use SNMP ACLs (firewalls) to help reduce SNMP's vulnerabilities, as SNMP traffic can be easily exploited to produce a denial of service (DoS).
    - <IP-SNMP-ACL-NAME> — Specify the SNMP IP ACL name. If the access list does not exist, it is created. After creating the SNMP ACL, define the deny/permit rules based on the network and/or host IP addresses. Once created and configured, link this SNMP IP ACL with a SNMP community string.

  **Note:** To link the SNMP community string with the SNMP IP ACL, in the management-policy-config-mode, use the following command: `snmp-server > community <COMMUNITY-STRING> > [ro|rw] > ip-snmp-access-list <IP-SNMP-ACL-NAME>`. 
Examples

rfs7000-37FABE(config)#ip access-list test
rfs7000-37FABE(config-ip-acl-test)#?

ACL Configuration commands:
- deny Specify packets to reject
- disable Disable rule if not needed
- no Negate a command or set its defaults
- permit Specify packets to forward

- clrscr Clears the display screen
- commit Commit all changes made in this session
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-ip-acl-test)#

rfs7000-37FABE(config)#ip snmp-access-list SNMPAcl
rfs7000-37FABE(config-ip-snmp-acl-SNMPAcl)#?

SNMP ACL Configuration commands:
- deny Specify packets to reject
- no Negate a command or set its defaults
- permit Specify packets to forward

- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- exit End current mode and change to EXEC mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-ip-snmp-acl-SNMPAcl)#

Related Commands

| no       | Removes an IP access control list |

NOTE: For more information on access control lists, see Chapter 11, ACCESS-LIST.
4.1.53 ipv6

▲ Global Configuration Commands

Creates a IPv6 ACL

An IPv6 ACL defines a set of rules that filter IPv6 packets flowing through a port or interface. Each rule specifies
the action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit,
the packet is allowed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX,
  AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530,
  NX9000, NX9500, NX9510, NX9600

Syntax

ipv6 access-list <IPv6-ACL-NAME>

Parameters

- ipv6 access-list <IPv6-ACL-NAME>

Examples

rfs4000-229D58 (config)#ipv6 access-list IPv6ACLTest
rfs4000-229D58 (config-ipv6-acl-IPv6ACLTest)#?
IPv6 Access Control Mode commands:
  deny Specify packets to reject
  no Negate a command or set its defaults
  permit Specify packets to forward
  clrscr Clears the display screen
  commit Commit all changes made in this session
  do Run commands from Exec mode
  end End current mode and change to EXEC mode
  exit End current mode and down to previous mode
  help Description of the interactive help system
  revert Revert changes
  service Service Commands
  show Show running system information
  write Write running configuration to memory or terminal

rfs4000-229D58 (config-ipv6-acl-IPv6ACLTest)#

Related Commands

- no Removes an IPv6 access control list

NOTE: For more information on access control lists, see Chapter 11, ACCESS-LIST.
4.1.54 *ipv6-router-advertisement-policy*

The following table lists the IPv6 *router advertisement* (RA) policy configuration commands:

<table>
<thead>
<tr>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
<th><strong>Reference</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-router-advertisement-policy</td>
<td>Creates a new IPv6 RA policy and enters its configuration mode</td>
<td>page 4-238</td>
</tr>
<tr>
<td>ipv6-router-advertisement-policy-mode commands</td>
<td>Summarizes the IPv6 RA policy configuration mode commands</td>
<td>page 4-240</td>
</tr>
</tbody>
</table>
4.1.54.1 ipv6-router-advertisement-policy

ipv6-router-advertisement-policy

Creates an IPv6 RA policy and enters its configuration mode

An IPv6 router policy allows routers to advertise their presence in response to solicitation messages. After receiving a neighbor solicitation message, the destination node sends an advertisement message, which includes the link layer address of the source node. After receiving the advertisement, the destination device replies with a neighbor advertisement message on the local link. After the source receives the advertisement it can communicate with other devices.

Advertisement messages are also sent to indicate a change in link layer address for a node on the local link. With such a change, the multicast address becomes the destination address for advertisement messages.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ipv6-router-advertisement-policy <POLICY-NAME>

Parameters

- ipv6-router-advertisement-policy <POLICY-NAME>

Examples

rfs4000-229D58(config)#ipv6-router-advertisement-policy test
rfs4000-229D58(config-ipv6-radv-policy-test)#?

IPv6 Router Advertisement Policy Mode commands:

- advertise
- assist-neighbor-discovery
- check-ra-consistency
- dns-server
- domain-name
- managed-config-flag
- nd-reachable-time
- no
- ns-interval
- other-config-flag
- ra
- router-lifetime
- router-preference
- unicast-solicited-advertisement

Enter the RA policy name. If the policy does not exist, it is created.
### Global Configuration Commands

- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **do**: Run commands from Exec mode
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal

```
rfs4000-229D58(config-ipv6-radv-policy-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the specified IPv6 RA policy</td>
</tr>
</tbody>
</table>
### 4.1.54.2 ipv6-router-advertisement-policy-mode commands

*ipv6-router-advertisement-policy*

The following table summarizes IPv6 router advertisement policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertise</td>
<td>Enables advertisement of IPv6 <em>maximum transmission unit</em> (MTU) and hop-count value in RAs</td>
<td>page 4-241</td>
</tr>
<tr>
<td>assist-neighbor-discovery</td>
<td>Enables advertisement of the source link layer address in RAs</td>
<td>page 4-242</td>
</tr>
<tr>
<td>check-ra-consistency</td>
<td>Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link</td>
<td>page 4-243</td>
</tr>
<tr>
<td>dns-server</td>
<td>Configures the DNS server’s IPv6 address and lifetime advertised in RAs</td>
<td>page 4-244</td>
</tr>
<tr>
<td>domain-name</td>
<td>Configures the Domain name search label advertised in RAs</td>
<td>page 4-245</td>
</tr>
<tr>
<td>managed-config-flag</td>
<td>Sets the managed address configuration flag in RAs</td>
<td>page 4-246</td>
</tr>
<tr>
<td>nd-reachable-time</td>
<td>Enables advertisement of neighbor reachable time in RAs</td>
<td>page 4-247</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts router advertisement policy settings</td>
<td>page 4-248</td>
</tr>
<tr>
<td>ns-interval</td>
<td>Configures the interval between two successive retransmitted <em>neighbor solicitation</em> (NS) messages</td>
<td>page 4-249</td>
</tr>
<tr>
<td>other-config-flag</td>
<td>Sets the other-configuration flag in RAs</td>
<td>page 4-250</td>
</tr>
<tr>
<td>ra</td>
<td>Configures RA related parameters, such as the interval between two unsolicited successive RAs</td>
<td>page 4-251</td>
</tr>
<tr>
<td>router-lifetime</td>
<td>Configures the default router’s lifetime, in seconds, advertised in RAs</td>
<td>page 4-252</td>
</tr>
<tr>
<td>router-preference</td>
<td>Configures the router preference field value advertised in RAs</td>
<td>page 4-253</td>
</tr>
<tr>
<td>unicast-solicited-advertisement</td>
<td>Enables unicasting of solicited RAs</td>
<td>page 4-254</td>
</tr>
</tbody>
</table>
4.1.54.2 advertise

ipv6-router-advertisement-policy-mode commands

Enables advertisement of IPv6 MTU and hop-count value in RAs

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

advertise [hop-limit|mtu]

Parameters

- advertise [hop-limit|mtu]

| advertise [hop-limit|mtu] | Enables advertisement of IPv6 MTU and hop-count value in RAs. Both these features are disabled by default. |

Examples

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#advertise hop-limit

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#advertise mtu

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
advertise mtu
advertise hop-limit

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

Related Commands

no | Enables advertisement of IPv6 MTU and hop-count value in RAs
assist-neighbor-discovery

ipv6-router-advertisement-policy-mode commands

Enables advertisement of the source link layer address in RAs to facilitate neighbor discovery. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
assist-neighbor-discovery

Parameters
None

Examples
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#assist-neighbor-discovery

Related Commands

| no | Enables the advertisement of the source link layer address in RAs |
4.1.54.2.3 check-ra-consistency

IPv6 router-advertisement-policy-mode commands

Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link. If the values advertised are inconsistent, a conflict is logged.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
check-ra-consistency
```

Parameters

None

Examples

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#check-ra-consistency
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context ipv6-router-advertisement-policy test advertise mtu advertise hop-limit check-ra-consistency
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#
```

Related Commands

| no | Disables comparison of interface-specific parameters advertised by other routers, within the link, with those advertised with this router |
4.15.4.2.4 dns-server

**ipv6-router-advertisement-policy-mode commands**

Configures the DNS server’s IPv6 address and lifetime. The configured values are advertised in RAs.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}

**Parameters**
- dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}

| dns-server <IPv6> | Configures the DNS server’s IPv6 address
| lifetime [<4-3600>|expired|infinite] | Enables the use of a DNS server to resolve host names to IPv6 addresses. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution.

|lifetime [<4-3600>| expired|infinite] | Optional. Configures the DNS server’s (identified by the <IPv6> parameter) lifetime
- <4-3600> – Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds.
- expired – Advertises that this DNS server’s lifetime has expired and should not be used
- infinite – Advertises that this DNS server’s lifetime is infinite

**Examples**

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#dns-server 2002::2 lifetime 3000

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

**Related Commands**

| no | Removes the DNS server settings advertised in RAs. Once removed these values are not advertised in RAs. |
4.1.54.2.5 domain-name

Configures the Domain name search label advertised in RAs.

Supported in the following platforms:
  • Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  • Wireless Controllers — RFS4000, RFS6000, RFS7000
  • Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

domain-name <WORD> {lifetime [<4-3600>|expired|infinite]}

Parameters
  • domain-name <WORD> {lifetime [<4-3600>|expired|infinite]}

| domain-name <WORD> | Configures the Domain name search label advertised in RAs. Enter a fully qualified domain name (FQDN), which is an unambiguous domain name available in a router advertisement resource. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com.
| lifetime [<4-3600>| expired|infinite] | Optional. Configures the Domain name search label's lifetime.
  • <4-3600> – Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds.
  • expired – Advertises that this Domain name search label's lifetime has expired and should not be used.
  • infinite – Advertises that this Domain name search label's lifetime is infinite.

Examples

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
  advertise mtu
  advertise hop-limit
  check-ra-consistency
dns-server 2002::2 lifetime 3000
  domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

Related Commands

| no | Removes the Domain name settings advertised in RAs. Once removed these values are not advertised in RAs. |
4.1.54.2.6 managed-config-flag

Sets the managed address configuration flag in RAs. When set, it indicates that IPv6 addresses are available through DHCPv6. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
managed-config-flag

Parameters
None

Examples
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#managed-config-flag
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
  managed-config-flag
  advertise mtu
  advertise hop-limit
  check-ra-consistency
  dns-server 2002::2 lifetime 3000
  domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the managed address configuration flag advertised in RAs</td>
</tr>
</tbody>
</table>
4.1.54.2.7  nd-reachable-time

Enables advertisement of neighbor discovery reachable time in RAs. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
nd-reachable-time [<5000-3600000>|global]
```

Parameters

- `nd-reachable-time [<5000-3600000>|global]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;5000-3600000&gt;</code></td>
<td>Configures an interface-specific value. Specify a value from 5000 - 3600000 milliseconds. The default is 5000 milliseconds.</td>
</tr>
<tr>
<td><code>global</code></td>
<td>Advertises the neighbor reachable time configured for the system. This is the value configured at the device configuration mode. For more information, see <code>ipv6</code>.</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#nd-reachable-time 6000
```

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
managed-config-flag
nd-reachable-time 6000
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#
```

Related Commands

```
no
```
Disables advertisement of neighbor reachable time in RAs
4.1.54.2.8 no

*ipv6-router-advertisement-policy-mode commands*

Removes or reverts router advertisement policy settings. Use the no command to remove or revert the interface-specific parameters that are advertised by link router.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [advertise [hop-limit|mtu]|assist-neighbor-discovery|check-ra-consistency|
dns-server <IPv6>|domain-name <WORD>|managed-config-flag|nd-reachable-time|\nns-interval|other-config-flag|ra [interval|suppress]|router-lifetime|
unicast-solicited-advertisement]
```

**Parameters**

- no

**Examples**

```plaintext
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
managed-config-flag
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#no managed-config-flag
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#no nd-reachable-time
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#no check-ra-consistency

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
advertise mtu
advertise hop-limit
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#
```

no <PARAMETERS> Removes or reverts this IPv6 router advertisement policy’s settings based on the parameters passed.
4.1.54.2.9 ns-interval

ipv6-router-advertisement-policy-mode commands

Configures the neighbor solicitation (NS) retransmit timer value advertised in RAs. This is the interval between two successive NS messages. When specified, it enables the sending of the specified value in RAs. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
ns-interval [<1000-3600000>|global]

Parameters
- ns-interval [<1000-3600000>|global]

| ns-interval [<1000-3600000]> | Configures the NS interval advertised in RAs. Use one of the following options:
|-------------------------------|---------------------------------------------------------------|
| global                        | • <1000-3600000> – Specify a value from 1000 - 3600000 milliseconds. The default is 1000 milliseconds.
|                               | • global – Advertises the NS interval configured for the system. This is configured on the device in the device configuration mode. For more information, see ipv6.

Examples
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#ns-interval 3000

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
managed-config-flag
nd-reachable-time global
ns-interval 3000
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

Related Commands

no Disables advertisement of NS interval in RAs
4.1.54.2.10  other-config-flag

Sets the other-configuration flag in RAs. When set, it indicates that other configuration details, such as DNS-related information, are available through DHCPv6. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
other-config-flag

Parameters
None

Examples
rfs7000-6DCD4B(config-ipv6-ra-radv-policy-test)#other-config-flag

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the other-config-flag advertised on RAs</td>
</tr>
</tbody>
</table>
4.1.54.2.11 ra

*ipv6-router-advertisement-policy-mode commands*

Configures RA related parameters, such as the interval between two unsolicited successive RAs. It also allows suppression of RAs.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
ra [interval <3-1800>|suppress]
```

**Parameters**
- `ra [interval <3-1800>|suppress]`

<table>
<thead>
<tr>
<th>interval &lt;3-1800&gt;</th>
<th>Configures the interval, in seconds, between two unsolicited successive RAs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;3-1800&gt;</td>
<td>Specify a value from 3 - 1800 seconds. The default is 300 seconds.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The router-lifetime should be at least three times the specified router interval.</td>
</tr>
</tbody>
</table>

| suppress | Enables the suppression of RAs. When enabled, the transmission of RAs in IPv6 packets is suppressed. This option is disabled by default. The `no > ra > suppress` command enables the sending of RAs. |

**Examples**
```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#ra interval 200
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#ra suppress
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context ipv6-router-advertisement-policy test
ra suppress
ra interval 200
managed-config-flag
nd-reachable-time global
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#
```

**Related Commands**
```
no
```

Removes the RA interval, and enables the sending of RAs.
4.1.54.2.12 router-lifetime

ipv6-router-advertisement-policy-mode commands

Configures the default router’s lifetime, in seconds, advertised in RAs

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
router-lifetime <0-9000>

Parameters
- router-lifetime <0-9000>

| router-lifetime <0-9000> | Configures the default router’s lifetime  
|--------------------------|-----------------------------------------------  
| <0-9000>                 | - <0-9000> – Specify a value from 0 - 9000 seconds. The default value is 1500 seconds. 
|                           | Note: A value of “0” indicates that this router is not the default router. |

Examples
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#router-lifetime 2000

rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
ra suppress
ra interval 200
managed-config-flag
nd-reachable-time global
router-lifetime 2000
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#

Related Commands
- no
  Removes the default router’s lifetime
4.1.54.2.13 router-preference

*ipv6-router-advertisement-policy-mode commands*

Configures the router preference field value advertised in RAs. The options are high, medium, and low. This value is used to prioritize and select the default router when multiple routers are discovered.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
router-preference [high|medium|low]
```

**Parameters**

- `router-preference [high|medium|low]`

---

| router-preference [high|medium|low] | Sets this router's preference over other routers, in the link, to be the default router. The options are high, low, and medium. The default value is medium. |
|--------------------------------------|------------------------------------------------------------------------------------------------|
| **Note:** The following points should be taken into consideration when configuring router preference: | |
| • For a router to be selected as a default router, the router's lifetime should not be equal to "0". | |
| • To enable default router selection, using router information contained in RAs, configure default router selection on that interface. | |

**Examples**

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#router-preference high
```

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
  ra suppress
  ra interval 200
  managed-config-flag
  nd-reachable-time global
  router-lifetime 2000
  advertise mtu
  advertise hop-limit
  router-preference high
  check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubbs lifetime infinite
```

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#
```
4.1.54.2.14 **unicast-solicited-advertisement**

*ipv6-router-advertisement-policy-mode commands*

Enables uncasting of solicited RAs. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
unicast-solicited-advertisement
```

**Parameters**

None

**Examples**

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#unicast-solicited-advertisement
```

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
    ra suppress
    ra interval 200
    unicast-solicited-advertisement
    managed-config-flag
    nd-reachable-time global
    router-lifetime 2000
    advertise mtu
    advertise hop-limit
    router-preference high
    check-ra-consistency
    dns-server 2002::2 lifetime 3000
    domain-name TechPubs lifetime infinite
```

```
rfs7000-6DCD4B(config-ipv6-radv-policy-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables uncasting of solicited RAs</td>
</tr>
</tbody>
</table>
4.1.55 l2tpv3

Global Configuration Commands

Configures a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel policy, used to create one or more L2TPv3 tunnels. The L2TPv3 policy defines the control and encapsulation protocols needed for tunneling layer 2 frames between two IP nodes. This policy enables creation of L2TPv3 tunnels for transporting Ethernet frames between bridge VLANs and physical GE ports. L2TPv3 tunnels can be created between any vendor devices supporting L2TPv3 protocol.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

l2tpv3 policy <L2TPV3-POLICY-NAME>

Parameters

- l2tpv3 policy <L2TPV3-POLICY-NAME>

Examples

rfs7000-37FABE(config)#l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#?

L2tpv3 Policy Mode commands:

- `cookie-size` – Size of the cookie field present in each l2tpv3 data message
- `failover-delay` – Time interval for re-establishing the tunnel after the failover (RF-Domain manager/VRRP-master/Cluster-master failover)
- `force-l2-path-recovery` – Enables force learning of servers, gateways etc., behind the l2tpv3 tunnel when the tunnel is established
- `hello-interval` – Configure the time interval (in seconds) between l2tpv3 Hello keep-alive messages exchanged in l2tpv3 control connection
- `no` – Negate a command or set its defaults
- `reconnect-attempts` – Maximum number of attempts to reestablish the tunnel.
- `reconnect-interval` – Time interval between the successive attempts to reestablish the l2tpv3 tunnel
- `retry-attempts` – Configure the maximum number of retransmissions for signaling message
- `retry-interval` – Time interval (in seconds) before the initiating a retransmission of any l2tpv3 signaling message
- `rx-window-size` – Number of signaling messages that can be received without sending the acknowledgement
- `tx-window-size` – Number of signaling messages that can be sent without receiving the acknowledgement

- `clrscr` – Clears the display screen
- `commit` – Commit all changes made in this session
- `end` – End current mode and change to EXEC mode
- `exit` – End current mode and down to previous mode
- `help` – Description of the interactive help system
- `revert` – Revert changes
- `service` – Service Commands
- `show` – Show running system information
write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an existing L2TPv3 tunnel policy</td>
</tr>
<tr>
<td>mint-policy</td>
<td>Configures the global MiNT policy</td>
</tr>
</tbody>
</table>

NOTE: For more information on the L2TPv3 tunnel configuration mode and commands, see Chapter 22, L2TPV3-POLICY.
4.1.56  mac

Global Configuration Commands

Configures a MAC ACLs

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

mac access-list <MAC-ACL-NAME>

Parameters

- mac access-list <MAC-ACL-NAME>

Examples

rfs7000-37FABE(config)#mac access-list test
rfs7000-37FABE(config-mac-acl-test)#?

MAC Extended ACL Configuration commands:
- deny Specify packets to reject
- disable Disable rule if not needed
- no Negate a command or set its defaults
- permit Specify packets to forward
- clrscr Clears the display screen
- commit Commit all changes made in this session
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-mac-acl-test)#

Related Commands

no Removes a MAC access control list

NOTE: For more information on MAC access control lists, see Chapter 11, ACCESS-LIST.
4.1.57 **management-policy**

*Global Configuration Commands*

Configures a management policy. Management policies include services that run on a device, welcome messages, banners etc.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
management-policy <MANAGEMENT-POLICY-NAME>
```

**Parameters**

- `management-policy <MANAGEMENT-POLICY-NAME>`

---

### Examples

```
<DEVICE>(config)#management-policy test
<DEVICE>(config-management-policy-test)#?
```

Management Mode commands:

- `aaa-login` Set authentication for logins
- `banner` Define a login banner
- `ftp` Enable FTP server
- `http` Hyper Text Terminal Protocol (HTTP)
- `https` Secure HTTP
- `idle-session-timeout` Configure idle timeout for a configuration session (GUI or CLI)
- `ipv6` IPv6 Protocol
- `no` Negate a command or set its defaults
- `privilege-mode-password` Set the password for entering CLI privilege mode
- `restrict-access` Restrict management access to the device
- `snmp-server` SNMP
- `ssh` Enable ssh
- `t5` T5 configuration
- `telnet` Enable telnet
- `user` Add a user account
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
<DEVICE>(config-management-policy-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes an existing management policy</td>
</tr>
</tbody>
</table>
NOTE: For more information on Management policy configuration, see Chapter 15, MANAGEMENT-POLICY.
### 4.1.58 meshpoint

**Global Configuration Commands**

Creates a new meshpoint and enters its configuration mode. Use this command to select and configure existing meshpoints.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
meshpoint [<MESHPOINT-NAME>|containing <WORD>]
```

**Parameters**

- `meshpoint [<MESHPOINT-NAME>|containing <WORD>]`

**Examples**

```plaintext
rfs7000-37FABE(config)#meshpoint TestMeshpoint
rfs7000-37FABE(config-meshpoint-TestMeshpoint)#?
```

**Mesh Point Mode commands:**

- `allowed-vlans` Set the allowed VLANs
- `beacon-format` The beacon format of this meshpoint
- `control-vlan` VLAN for meshpoint control traffic
- `data-rates` Specify the 802.11 rates to be supported on this meshpoint
- `description` Configure a description of the usage of this meshpoint
- `force` Force suboptimal paths
- `meshid` Configure the Service Set Identifier for this meshpoint
- `neighbor` Configure neighbor specific parameters
- `no` Negate a command or set its defaults
- `root` Set this meshpoint as root
- `security-mode` The security mode of this meshpoint
- `shutdown` Shutdown this meshpoint
- `use` Set setting to use
- `wpa2` Modify ccmp wpa2 related parameters

```plaintext
rfs7000-37FABE(config-meshpoint-TestMeshpoint)#
```

**Related Commands**

- `no` Removes an existing meshpoint
NOTE: For more information on Meshpoint configuration, see Chapter 26, MESHPOINT.
4.1.59 **meshpoint-qos-policy**

- **Global Configuration Commands**

Configures a set of parameters that defines the meshpoint quality of service (QoS) policy

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

**Parameters**

- `meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>`

**Examples**

```
rfs7000-37FABE(config)#meshpoint-qos-policy TestMeshpointQoS
rfs7000-37FABE(config-meshpoint-qos-TestMeshpointQoS)#?
```

Mesh Point QoS Mode commands:

- `accelerated-multicast` Configure accelerated multicast streams address and forwarding QoS classification
- `no` Negate a command or set its defaults
- `rate-limit` Configure traffic rate-limiting parameters on a per-meshpoint/per-neighbor basis

- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-meshpoint-qos-TestMeshpointQoS)#
```

**Related Commands**

- `no` Removes an existing meshpoint QoS policy

---

**NOTE:** For more information on Meshpoint QoS policy configuration, see Chapter 26, MESHPOINT.
4.1.60 mint-policy

> Global Configuration Commands

Configures the global MiNT policy

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

mint-policy global-default

Parameters

- mint-policy global-default

| global-default | Configures the global default MiNT policy |

Examples

rfs7000-37FABE(config)#mint-policy global-default
rfs7000-37FABE(config-mint-policy-global-default)#?
Mint Policy Mode commands:
  level Mint routing level
  mtu Configure the global Mint MTU
  no Negate a command or set its defaults
  router Mint router
  udp Configure mint UDP/IP encapsulation
  clrscr Clears the display screen
  commit Commit all changes made in this session
  do Run commands from Exec mode
  end End current mode and change to EXEC mode
  exit End current mode and down to previous mode
  help Description of the interactive help system
  revert Revert changes
  service Service Commands
  show Show running system information
  write Write running configuration to memory or terminal

rfs7000-37FABE(config-mint-policy-global-default)#

Related Commands

| no | Removes an existing MiNT policy |

NOTE: For more information on MiNT policy configuration, see Chapter 14, MINT-POLICY.
4.1.61 nac-list

A Network Access Control (NAC) policy configures a list of devices that can access a network based on their MAC addresses.

The following table lists NAC list configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>nac-list</td>
<td>Creates a NAC list and enters its configuration mode</td>
<td>page 4-265</td>
</tr>
<tr>
<td>nac-list-mode commands</td>
<td>Summarizes NAC list configuration mode commands</td>
<td>page 4-266</td>
</tr>
</tbody>
</table>
4.1.61.1 nac-list

 Configures a NAC list that manages access to the network

 Supported in the following platforms:

 - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
 - Wireless Controllers — RFS4000, RFS6000, RFS7000
 - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

 Syntax

 nac-list <NAC-LIST-NAME>

 Parameters

 - nac-list <NAC-LIST-NAME>

 Examples

 rfs7000-37FABE(config)#nac-list test
 rfs7000-37FABE(config-nac-list-test)#?

 NAC List Mode commands:

 - exclude Specify MAC addresses to be excluded from the NAC enforcement list
 - include Specify MAC addresses to be included in the NAC enforcement list
 - no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

 rfs7000-37FABE(config-nac-list-test)#

 Related Commands

 no Removes a NAC list
4.1.61.2 nac-list-mode commands

The following table summarizes NAC list configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specifies the MAC addresses excluded from the NAC enforcement list</td>
<td>page 4-267</td>
</tr>
<tr>
<td>include</td>
<td>Specifies the MAC addresses included in the NAC enforcement list</td>
<td>page 4-268</td>
</tr>
<tr>
<td>no</td>
<td>Cancels an exclude or include NAC list rule</td>
<td>page 4-269</td>
</tr>
</tbody>
</table>
4.1.61.2.1 exclude

nac-list-mode commands

Specifies the MAC addresses excluded from the NAC enforcement list

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

Syntax
exclude <START-MAC> [<END-MAC> precedence <1-1000> | precedence <1-1000>]

Parameters
- exclude <START-MAC> [<END-MAC> precedence <1-1000> | precedence <1-1000>]

| <START-MAC> | Specifies a range of MAC addresses or a single MAC address to exclude from the NAC enforcement list
| --- | --- |
| • <START-MAC> | Specify the first MAC address in the range.
| Note: Use this parameter to specify a single MAC address.

| <END-MAC> | Specifies the last MAC address in the range (optional if a single MAC is added to the list)
| --- | --- |
| • <END-MAC> | Specify the last MAC address in the range.

| precedence <1-1000> | Sets the rule precedence. Exclude entries are checked in the order of their rule precedence.
| --- | --- |
| • <1-1000> | Specify a value from 1 - 1000.

Examples
rfs7000-37FABE(config-nac-list-test)#exclude 00-40-96-B0-BA-2A precedence 1

rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
  exclude 00-40-96-B0-BA-2A 00-40-96-B0-BA-2A precedence 1
rfs7000-37FABE(config-nac-list-test)#
4.1.61.2.2 include

* nac-list-mode commands

Specifies the MAC addresses included in the NAC enforcement list

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
include <START-MAC> [ <END-MAC> precedence <1-1000> | precedence <1-1000> ]

Parameters
- include <START-MAC> [ <END-MAC> precedence <1-1000> | precedence <1-1000> ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;START-MAC&gt;</td>
<td>Specifies a range of MAC addresses or a single MAC address to include in the NAC enforcement list</td>
</tr>
<tr>
<td></td>
<td>• &lt;START-MAC&gt; – Specify the first MAC address in the range.</td>
</tr>
<tr>
<td>Note:</td>
<td>Use this parameter to specify a single MAC address.</td>
</tr>
<tr>
<td>&lt;END-MAC&gt;</td>
<td>Specifies the last MAC address in the range (optional if a single MAC is added to the list)</td>
</tr>
<tr>
<td></td>
<td>• &lt;END-MAC&gt; – Specify the last MAC address in the range.</td>
</tr>
<tr>
<td>precedence &lt;1-1000&gt;</td>
<td>Sets the rule precedence. Include entries are checked in the order of their rule precedence.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-1000&gt; – Specify a value from 1 - 1000.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-nac-list-test)#include 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
  exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
  include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#
4.1.61.2.3 no

- nac-list-mode commands

Cancels an exclude or include NAC list rule

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9560

Syntax

no [exclude|include]

no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]

Parameters

- no <PARAMETERS>

Examples

The following example shows the NAC list ‘test’ settings before the ‘no’ command is executed:

rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
  exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
  include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#

rfs7000-37FABE(config-nac-list-test)#no exclude 00-40-96-B0-BA-2A precedence 1

The following example shows the NAC list ‘test’ settings after the ‘no’ command is executed:

rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
  include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#

Related Commands

<table>
<thead>
<tr>
<th>exclude</th>
<th>Specifies MAC addresses excluded from the NAC enforcement list</th>
</tr>
</thead>
<tbody>
<tr>
<td>include</td>
<td>Specifies MAC addresses included in the NAC enforcement list</td>
</tr>
</tbody>
</table>
4.1.62 no

Global Configuration Commands

Negates a command, or reverts configured settings to their default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax


no application <APPLICATION-NAME>

no [ap621|ap622|ap650|ap651|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap82xx|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600]<MAC>

no client-identity <CLIENT-IDENTITY-NAME>

no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>

no device {containing <WORD>} {[/filter type [ap621|ap622|ap650|ap651|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|ap82xx|ex3524|ex3548|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600]}

no password-encryption secret 2 <OLD-PASSPHRASE>

no profile {ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap81xx|ap82xx|ex3524|ex3548|containing|filter|nx45xx|nx5500|nx65xx|nx75xx|
nx9000|nx9600|t5|vx9000} <PROFILE-NAME>

no wlan [<WLAN-NAME>|all|containing <WLAN-NAME-SUBSTRING>]

no service set [command-history|reboot-history|upgrade-history] {on <DEVICE-NAME>}

The following 'no' commands are specific to the RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, and NX9000 platforms:

no t5 <T5-DEVICE-MAC>

The following 'no' commands are specific to the RFS4000, RFS6000, NX45XX, NX65XX, and NX9000 platforms:

no bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list]

The following 'no' commands are specific to the NX45XX, NX65XX, NX9000 series service platforms:

no smart-cache-policy <SMART-CACHE-POLICY-NAME>

no route-map <ROUTE-MAP-NAME>

The following 'no' commands are specific to the AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP8132, RFS4000, RFS6000, RFS7000, NX45XX and NX65XX platforms:

no url-filter <URL-FILTER-NAME>

The following 'no' command is specific to the NX9000 series service platforms:

no vx9000 <VX9000-MAC>

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes or resets settings, configurable in the global configuration mode, based on the parameters passed |

Examples

<DEVICE>(config)#no ?

aaa-policy Delete a aaa policy
aaa-tacacs-policy Delete a aaa tacacs policy
alias Alias
ap621 Delete an AP621 access point
ap622 Delete an AP622 access point
ap650 Delete an AP650 access point
ap6511 Delete an AP6511 access point
ap6521 Delete an AP6521 access point
ap6522 Delete an AP6522 access point
ap6532 Delete an AP6532 access point
ap6562 Delete an AP6562 access point
ap71xx Delete an AP71XX access point
ap7502 Delete an AP7502 access point
ap7522 Delete an AP7522 access point
ap7532 Delete an AP7532 access point
ap7562 Delete an AP7562 access point
ap81xx Delete an AP81XX access point
ap82xx Delete an AP82XX access point
application Delete an application
application-policy Delete an application policy
association-acl-policy Delete an association-acl policy
auto-provisioning-policy Delete an auto-provisioning policy
bgp BGP Configuration
bonjour-gw-discovery-policy
bonjour-gw-forwarding-policy
bonjour-gw-query-forwarding-policy
captive-portal
client-identity
client-identity-group
cryptocmp-policy
customize
device
device-categorization
dhcps-server-policy
dhcpsv6-server-policy
dns-whitelist
event-system-policy
ex3500
ex3500-management-policy
ex3500-qos-class-map-policy
ex3500-qos-policy-map
ex3524
ex3548
firewall-policy
global-association-list
guest-management
igmp-snoop-policy
inline-password-encryption
ip
ipv6
ipv6-router-advertisement-policy
l2tpv3
mac
management-policy
meshpoint
meshpoint-qos-policy
nac-list
nsight-policy
nx45xx
nx5500
nx65xx
nx75xx
nx9000
passpoint-policy
password-encryption
profile
radio-qos-policy
radius-group
radius-server-policy
radius-user-pool-policy
rf-domain
rf4000
rf6000
rf7000
roaming-assist-policy
role-policy
route-map
routing-policy
smart-cache-policy
smart-rf-policy

bonjour-gw-discovery-policy Disable Bonjour Gateway discovery policy
bonjour-gw-forwarding-policy Disable Bonjour Gateway Forwarding policy
bonjour-gw-query-forwarding-policy Disable Bonjour Gateway Query Forwarding policy
captive-portal Delete a captive portal
client-identity Client identity (DHCP Device Fingerprinting)
client-identity-group Client identity group (DHCP Fingerprint Database)
cryptocmp-policy CMP policy
customize Restore the custom cli commands to default
device Delete multiple devices
device-categorization Delete device categorization object
dhcps-server-policy DHCP server policy
dhcpsv6-server-policy DHCPv6 server related configuration
dns-whitelist Delete a whitelst object
event-system-policy Delete a event system policy
ex3500 EX3500 device
ex3500-management-policy Delete a ex3500 management policy
ex3500-qos-class-map-policy Delete a ex3500 qos class-map policy
ex3500-qos-policy-map Delete a ex3500 qos policy-map
ex3524 Delete an EX3524 wireless controller
ex3548 Delete an EX3548 wireless controller
firewall-policy Configure firewall policy
global-association-list Delete a global association list
guest-management Delete a guest management policy
igmp-snoop-policy Remove device onboard igmp snoop policy
inline-password-encryption Disable storing encryption key in the startup configuration file
ip Internet Protocol (IP)
ipv6 Internet Protocol version 6 (IPv6)
ipv6-router-advertisement-policy IPv6 Router Advertisement related configuration
l2tpv3 Negate a command or set its defaults
mac MAC configuration
management-policy Delete a management policy
meshpoint Delete a meshpoint object
meshpoint-qos-policy Delete a mesh point QoS configuration policy
nac-list Delete an network access control list
nsight-policy Delete a nsight policy
nx45xx Delete an NX45XX integrated services platform
nx5500 Delete an NX5500 wireless controller
nx65xx Delete an NX65XX integrated services platform
nx75xx Delete an NX75XX wireless controller
nx9000 Delete an NX9000 wireless controller
passpoint-policy Delete a passpoint configuration policy
password-encryption Disable password encryption in configuration
profile Delete a profile and all its associated configuration
radio-qos-policy Delete a radio QoS configuration policy
radius-group Local radius server group configuration
radius-server-policy Remove device onboard radius policy
radius-user-pool-policy Configure Radius User Pool
rf-domain Delete one or more RF-domains and all their associated configurations
rf4000 Delete an RFS4000 wireless controller
rf6000 Delete an RFS6000 wireless controller
rf7000 Delete an RFS7000 wireless controller
roaming-assist-policy Delete a roaming-assist policy
role-policy Role based firewall policy
route-map Dynamic routing route map Configuration
routing-policy Policy Based Routing Configuration
smart-cache-policy Delete a content caching
smart-rf-policy Delete a smart-rf-policy
t5                                  Delete an T5 wireless controller
url-filter                          Delete a url filter
url-list                            Delete a URL list
vx9000                              Delete an VX9000 wireless controller
web-filter-policy                   Delete a web filter policy
wips-policy                         Delete a wips policy
wlan                                Delete a wlan object
wlan-qos-policy                     Delete a wireless lan QoS configuration policy

service                              Service Commands
<DEVICE>(config)#
4.1.63 nsight-policy

The following table lists NSight policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsight-policy</td>
<td>Creates an NSight policy and enters its configuration mode</td>
<td>page 4-275</td>
</tr>
<tr>
<td>nsight-policy</td>
<td>Summarizes NSight policy configuration mode commands</td>
<td>page 4-278</td>
</tr>
</tbody>
</table>
4.1.63.1 nsight-policy

*nsight-policy*

Creates an NSight policy and enters its configuration mode

The NSight policy is an advance management, analytics, reporting, and troubleshooting tool, which when created and applied at the RF Domain level allows the RF Domain manager to send statistics (polled from devices within the RF Domain) to the NOC. The NOC, when enabled as the NSight server, stores this data in a locally or externally hosted MongoDB database. This large, complex data are collated and presented on the NOC’s GUI in visual forms that are easy to understand and manage. For large networks, enabling NSight removes the inadequacies of the existing data collection, presentation, and analytics framework.

The WING NSight implementation consists of the following components:

- An NSight server hosted on the NOC
- A MongoDB database hosted on the NOC. This database consists of AP statistics gathered by RF Domain managers.
- An NSight UI application running on the NOC
- An NSight client hosted on the RF Domain manager. This is the SSM statistics module that periodically gathers statistics from adopted APs and forwards to the NSight server.

---

**NOTE:** NSight is a licensed option. To enable the NSight, navigate to the NSight server’s device configuration mode and apply the NSight license.

---

To enable NSight, follow the steps given below:

1. Create an NSight policy to enable the NSight server.
   
   ```
   nx9500-6C8809(config-nsight-policy-nsight-for-noc)#enable
   nx9500-6C8809(config-nsight-policy-nsight-for-noc)#nsight-server
   nx9500-6C8809(config-nsight-policy-nsight-for-noc)#show context
   nsight-policy nsight-for-noc
   nsight-server
   nx9500-6C8809(config-nsight-policy-nsight-for-noc)#
   ```

2. Apply the policy configured in step 1 to the NOC. This enables the NOC to recognize itself as the NSight server.
   
   ```
   nx9500-6C8809(config)#self
   nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#use nsight-policy nsight-for-noc
   ```

3. Create another NSight policy pointing to the NSight server host.
   
   ```
   nx9500-6C8809(config-nsight-policy-nsight-for-rfdm)#enable
   nx9500-6C8809(config-nsight-policy-nsight-for-rfdm)#server host 192.168.13.13
   nx9500-6C8809(config-nsight-policy-nsight-for-rfdm)#show context
   nsight-policy nsight-for-rfdm
   server host 192.168.13.13 https
   ```

4. Apply the policy configured in step 3 to the RF Domain. This enables the domain manager to collect statistics from the access points and send to the NOC serving as the NSight server.
   
   ```
   nx9500-6C8809(config)#rf-domain TechPubs
   nx9500-6C8809(config-rf-domain-TechPubs)#use nsight-policy nsight-for-rfdm
   ```

---

**NOTE:** NSight is a licensed option. To enable the NSight, navigate to the NSight server’s device configuration mode and apply the NSight license.
The NOC stores the statistical data, received from RF Domain managers, in the MongoDB database. This data contains following information:

- Operating parameters of devices – Fixed information of devices, such as IP addresses, wired interface status, radio operating parameters (channel, power etc.)
- SMART RF neighbor information – SMART RF neighbors' data for every radio. This data is used to generate and display heat-maps on floor map. Any changes in the SMART RF data is reported to the MART server and stored in the database.
- Rogue AP information – Rogue AP list and rogue AP status. Any changes in the rouge AP list or status is reported to the MART server and stored in the database.
- Wireless client list – Details of wireless clients within the RF Domain
- Wireless access point statistics – Statistics of all the APs in the RF Domain. AP statistics includes details, such as number of bytes transferred since the last reporting interval, number of TX retries, signal-noise-ratio (SNR), noise, RF quality index, client count etc.
- Wireless client statistics – Statistics of all the wireless clients in the RF Domain. Wireless client statistics includes details, such as number of bytes transferred from last reporting interval, number of TX retries, SNR, RF quality index etc.
- Wired interface statistics – Statistics of wired interfaces of all APs. It includes details, such as interface status, number of bytes transferred from last reporting interval etc.
- Event history – Event details for all APs adopted by the NOC. These are events received by the Cfgd every 30 seconds and sent to the MART server. Each event consists of the RF Domain name, wireless client MAC if applicable, AP MAC, event mnemonic, event timestamp, and the event string itself.

Apart from the above mentioned data, the MongoDB database contains information that is reported to the NSight server by the Cfgd running on the NOC. These are:

- Device information – Information of all devices (APs and controllers) within the network, such as hostname, device type, firmware version, location, geo-coordinates etc. This information is collected and reported by the Cfgd running on the NOC.
- Configuration elements, such as RF Domains, RF Domain location hierarchy, WLANs.

**NOTE:** All network devices (APs and controllers) should be upgraded to the latest WiNG build for NSight and MongoDB implementation.

Supported in the following platforms:
- Service Platforms — NX7500, NX9500, NX9510, NX9600

**Syntax**

```plaintext
nsight-policy <NSIGHT-POLICY-NAME>
```

**Parameters**

- `nsight-policy <NSIGHT-POLICY-NAME>`

| `<NSIGHT-POLICY-NAME>` | Specify the NSight policy name. If the policy does not exist, it is created. |
Examples

```
nx9500-6C8809(config)#nsight-policy test
nx9500-6C8809(config-nsight-policy-test)#?
Nsight Policy Mode) commands:
    enable         Enable this Nsight policy
    no             Negate a command or set its defaults
    nsight-server  Enable Nsight server functionality
    server         Configure Nsight server
    clrscr         Clears the display screen
    commit         Commit all changes made in this session
    exit           End current mode and down to previous mode
    help           Description of the interactive help system
    revert         Revert changes
    service        Service Commands
    show           Show running system information
    write          Write running configuration to memory or terminal
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes an existing NSight policy</td>
</tr>
</tbody>
</table>
### nsight-policy commands

The following table summarizes NSight policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables this NSight policy</td>
<td>page 4-279</td>
</tr>
<tr>
<td>nsight-server</td>
<td>Enables NSight server functionality and configures the SMTP report delivery</td>
<td>page 4-280</td>
</tr>
<tr>
<td>server</td>
<td>Configures the NSight server host. This configuration is used by the NSight</td>
<td>page 4-281</td>
</tr>
<tr>
<td></td>
<td>client to identify the NSight server host.</td>
<td></td>
</tr>
<tr>
<td>no</td>
<td>Removes this NSight policy settings</td>
<td>page 4-282</td>
</tr>
</tbody>
</table>
### 4.1.63.2.1 enable

#### nsight-policy commands

Enables this NSight policy. The default setting is enabled.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

```
enable
```

**Parameters**

None

**Examples**

```
nx9510-6C8A5C(config-nsight-policy-test2)#enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables this NSight policy</td>
</tr>
</tbody>
</table>
### 4.1.63.2.2 nsight-server

#### nsight-policy commands

Enables NSight server functionality and configures the SMTP report delivery settings. When applied to a device (NOC), this policy enables the device to recognize itself as the NSight server.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

#### Syntax

```
nsight-server {smtp-report-delivery host <WORD> sender <EMAIL-ADD> [port <1-65535>|
  security [none|ssl|starttls]|username <USER-NAME> password [0|2|<WORD>]]
```

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsight-server</td>
<td>Enables NSight server functionality on the host using this NSight policy</td>
</tr>
</tbody>
</table>
| smtp-report-delivery host <WORD> | Optional. Configures SMTP report delivery settings  
  |  • host <WORD> – Configures the SMTP server host  
  |  • <WORD> – Specify the SMTP server host’s IP address or hostname.  |
| sender <EMAIL-ADD> | Optional. Configures the SMTP sender’s e-mail address  
  |  • <EMAIL-ADD> – Specify the sender’s e-mail address.  |
| port <1-65535> | Optional. Configures the SMTP server port  
  |  • <1-65535> – Specify the port from 1 - 65535.  |
| security [none|ssl|starttls] | Optional. Configures the encryption protocol used by the SMTP server. The options are:  
  |  • none – Uses no encryption  
  |  • ssl – Uses SSL encryption  
  |  • starttls – Uses STARTTLS encryption  |
| username <USER-NAME> password [0|2|<WORD>] | Optional. Configures the SMTP username  
  |  • <USER-NAME> Specify the user name  
  |  • password [0|2|<WORD>] – Configures the password associated with the above configured user  
  |  • 0 – Configures a clear text password  
  |  • 2 – Configures an encrypted password  
  |  • <WORD> – Enter the password.  |

#### Examples

```
nx9510-6C8A5C(config-nsight-policy-test2)#nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#show context nsight-policy test2
nx9510-6C8A5C(config-nsight-policy-test2)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables NSight server functionality on this NSight policy</td>
</tr>
</tbody>
</table>
4.1.63.2.3 server

nsight-policy commands

Configures the NSight server host. This configuration is used by the NSight client to identify the NSight server host.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

Syntax

server host [<IP>|<HOSTNAME>|<X:X::X:X>] {http|https}

Parameters

- server host [<IP>|<HOSTNAME>|<X:X::X:X>] {http|https}

Examples

nx9510-6C8A5C(config-nsight-policy-test2)#server host 172.22.0.153 http

nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
server host 172.22.0.153 http
nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#

Related Commands

no

Removes NSight server host settings from this NSight policy
4.1.63.2.4  **no**

nsight-policy commands

Removes NSight policy settings

Supported in the following platforms:

- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [enable|nsight-server {smtp-report-delivery}|server host [<IP>|<HOSTNAME>|<X:X::X:]]
```

**Parameters**

- no <PARAMETERS>

---

**Examples**

The following example shows the NSight policy ‘test2’ settings before the ‘no’ command is executed:

```plaintext
nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
server host 172.22.0.153 http
nsight-server
```

```
nx9510-6C8A5C(config-nsight-policy-test2)#
```

```
nx9510-6C8A5C(config-nsight-policy-test2)#no server host 172.22.0.153
```

The following example shows the NSight policy ‘test2’ settings after the ‘no’ command is executed:

```
nx9500-6C8809(config-nsight-policy-test2)#show context
nsight-policy test2
nsight-server
```

```
nx9510-6C8A5C(config-nsight-policy-test2)#
```
4.1.64 passpoint-policy

Global Configuration Commands

Creates a new passpoint policy and enters its configuration mode.

The passpoint policy implements the Hotspot 2.0 Wi-Fi Alliance standard, enabling interoperability between clients, infrastructure, and operators. It makes a portion of the IEEE 802.11u standard mandatory and adds Hotspot 2.0 extensions that allow clients to query a network before actually attempting to join it.

The passpoint policy allows a single or set of Hotspot 2.0 configurations to be global and referenced by the devices that use it. It is mapped to a WLAN. However, only primary WLANs on a BSSID will have their passpoint policy configuration used.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
passpoint-policy <POLICY-NAME>

Parameters

- passpoint-policy <POLICY-NAME>

Examples
rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#?

Passpoint Policy Mode commands:
- 3gpp
- access-network-type
- connection-capability
- domain-name
- hessid
- internet
- ip-address-type
- nai-realm
- net-auth-type
- no
- operator
- osu
- roam-consortium
- venue
- wan-metrics

clrscr
commit
do
deret
exit
help
revert
service
show
write

rfs4000-229D58(config-passpoint-policy-test)#
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an existing passpoint policy</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on passpoint policy, see *Chapter 27, PASSPOINT POLICY.*
4.1.65 **password-encryption**

*Global Configuration Commands*

Enables password encryption

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
password-encryption secret 2 <LINE>
```

**Parameters**

- `secret 2 <LINE>`

<table>
<thead>
<tr>
<th>secret 2 &lt;LINE&gt;</th>
<th>Encrypts passwords with a secret phrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 – Specifies the encryption type as either SHA256 or AES256</td>
<td></td>
</tr>
<tr>
<td>&lt;LINE&gt; – Specify the encryption passphrase.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#password-encryption secret 2 example_company
```

**Related Commands**

| no | Disables password encryption |
4.1.66 profile

- **Global Configuration Commands**

  Configures profile related commands. If no parameters are given, all profiles are selected.

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
profile {anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|containing|filter|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600}

profile {anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600}

profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600]}

profile {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600]}
```

**Parameters**

- **profile {anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|containing|filter|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600}**
  - Configures device profile commands. If no device profile is specified, the system configures all device profiles.
  - **<DEVICE-TYPE>** – Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, and NX9600. After specifying the device type, specify the profile name.
  - **<DEVICE-PROFILE-NAME>** – Specify the profile name.

- **profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600]}
  - Optional. Configures profiles that contain a specified sub-string in the hostname

- **profile {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600]}
  - Optional. Configures profiles that contain a specified sub-string in the profile name to filter profiles.
### Global Configuration Commands

**filter type** | Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles.
---|---
| • type – Filters profiles by the device type. Select a device type from the following options: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, and NX9600.

Note: The NX9600 profile option is only available on an NX9600 device.

| profile | Configures device profile commands
---|---
| filter type | Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles.
| • type – Filters profiles by the device type. Select a device type from the following options: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, and NX9600.

Note: The NX9600 profile option is only available on an NX9600 device.

### Examples

```bash
<DEVICE> (config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE> (config-profile-<PROFILE-NAME>)#?
```

Profile Mode commands:
- **adopter-auto-provisioning-policy-lookup** | Use centralized auto-provisioning policy when adopted by another controller
- **adoption** | Adoption configuration
- **alias** | Alias
- **application-policy** | Application Policy configuration
- **area** | Set name of area where the system is located
- **arp** | Address Resolution Protocol (ARP)
- **auto-learn-staging-config** | Enable learning network configuration of the devices that come for adoption
- **autogen-uniqueid** | Autogenerate a unique id
- **autoinstall** | Autoinstall settings
- **bluetooth-detection** | Detect Bluetooth devices using the Bluetooth USB module
- **bridge** | Ethernet bridge
- **captive-portal** | Captive portal
- **cdp** | Cisco Discovery Protocol
- **cluster** | Cluster configuration
- **configuration-persistence** | Enable persistence of configuration across reboots (startup config file)
- **controller** | WLAN controller configuration
- **critical-resource** | Critical Resource
- **crypto** | Encryption related commands
- **database-backup** | Scheduled Database Backup
- **device-upgrade** | Device firmware upgrade
- **dot1x** | 802.1X
- **dpi** | Enable Deep-Packet-Inspection (Application Assurance)
- **dscp-mapping** | Configure IP DSCP to 802.1p priority mapping for untagged frames
- **email-notification** | Email notification configuration
- **enforce-version** | Check the firmware versions of devices before interoperating
- **environmental-sensor** | Environmental Sensors Configuration
events
export
file-sync
floor
gre
http-analyze
interface
ip
ipv6
l2tpv3
l3e-lite-table
led
led-timeout
legacy-auto-downgrade
legacy-auto-update
lldp
load-balancing
logging
mac-address-table
mac-auth
memory-profile
meshpoint-device
meshpoint-monitor-interval
min-misconfiguration-recovery-time
mint
misconfiguration-recovery-time
neighbor-inactivity-timeout
neighbor-info-interval
no
noc
ntp
offline-duration
power-config
preferred-controller-group
preferred-tunnel-controller
radius
raid
remove-override
rf-domain-manager
router
slot
spanning-tree
traffic-class-mapping
traffic-shape
trustpoint
tunnel-controller

System event messages
Export a file
File sync between controller and adoptees
Set the floor within a area where the system is located
GRE protocol
Specify HTTP-Analysus configuration
Select an interface to configure
Internet Protocol (IP)
Internet Protocol version 6 (IPv6)
L2tpv3 protocol
L3e lite Table
Turn LEDs on/off on the device
Configure the time for the led to turn off after the last radio state change
Enable device firmware to auto downgrade when other legacy devices are detected
Auto upgrade of legacy devices
Link Layer Discovery Protocol
Configure load balancing parameter
Modify message logging facilities
MAC Address Table
Memory profile to be used on the device
Configure meshpoint device parameters
Configure meshpoint monitoring interval
Check controller connectivity after configuration is received
MiNT protocol
Check controller connectivity after configuration is received
Configure neighbor inactivity timeout
Configure neighbor information exchange interval
Negate a command or set its defaults
Configure the noc related setting
Ntp server WORD
Set duration for which a device remains unadopted before it generates offline event
Configure power mode
Controller group this system will prefer for adoption
Tunnel Controller Name this system will prefer for tunneling extended vlan traffic
Configure device-level radius authentication parameters
RAID
Remove configuration item override from the device (so profile value takes effect)
RF Domain Manager
Dynamic routing
PCI expansion Slot
Spanning tree
Configure IPv6 traffic class to 802.1p priority mapping for untagged frames
Traffic shaping
Assign a trustpoint to a service
Tunnel Controller group this
GLOBAL CONFIGURATION COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>controller belongs to</td>
</tr>
<tr>
<td>vrrp</td>
<td>Set setting to use</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>VRRP configuration</td>
</tr>
<tr>
<td></td>
<td>Publish interface via OSPF/BGP only</td>
</tr>
<tr>
<td></td>
<td>if the interface VRRP state is not BACKUP</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enable support for 802.11 WEP</td>
</tr>
<tr>
<td></td>
<td>shared key authentication</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

<DEVICE>(config-profile-<PROFILE-NAME>)#

NOTE: For more information on profiles and how to configure profiles, see Chapter 7, PROFILES.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes a profile and its associated configurations</td>
</tr>
</tbody>
</table>
**4.1.67 radio-qos-policy**

*Global Configuration Commands*

Configures a radio quality-of-service (QoS) policy

Supported in the following platforms:
- Wireless Controllers — RFS4011

**Syntax**

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

**Parameters**

- `radio-qos-policy <RADIO-QOS-POLICY-NAME>`

---

<table>
<thead>
<tr>
<th><code>&lt;RADIO-QOS-POLICY-NAME&gt;</code></th>
<th>Specify the radio QoS policy name. If the policy does not exist, it is created.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config)#radio-qos-policy test
rfs7000-37FABE(config)#radio-qos-policy test?
```

Radio QoS Mode commands:

- `accelerated-multicast` Configure multicast streams for acceleration
- `admission-control` Configure admission-control on this radio for one or more access categories
- `no` Negate a command or set its defaults
- `smart-aggregation` Configure smart aggregation parameters
- `wmm` Configure 802.11e/Wireless MultiMedia parameters

- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-radio-qos-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th><code>no</code></th>
<th>Removes an existing Radio QoS policy</th>
</tr>
</thead>
</table>

---

**NOTE:** For more information on radio qos policy, see *Chapter 17, RADIO-QOS-POLICY.*
4.1.68 radius-group

Global Configuration Commands

Configures RADIUS user group parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

radius-group <RADIUS-GROUP-NAME>

Parameters

- radius-group <RADIUS-GROUP-NAME>

Examples

rfs7000-37FABE(config)#radius-group testgroup
rfs7000-37FABE(config-radius-group-testgroup)#?

Radius user group configuration commands:

- guest Make this group a Guest group
- no Negate a command or set its defaults
- policy Radius group access policy configuration
- rate-limit Set rate limit for group
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-group-testgroup)#

Related Commands

- no Removes an existing RADIUS group

NOTE: For more information on RADIUS user group commands, see Chapter 16, RADIUS-POLICY.
4.1.69 radius-server-policy

**Global Configuration Commands**

Creates an onboard device RADIUS policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

radius-server-policy <RADIUS-SERVER-POLICY-NAME>

**Parameters**

- radius-server-policy <RADIUS-SERVER-POLICY-NAME>

**Examples**

```bash
rfs7000-37FABE(config)#radius-server-policy testpolicy
rfs7000-37FABE(config-radius-server-policy-testpolicy)#?
```

**Radius Configuration commands:**

- **authentication**  
  Radius authentication
- **bypass**  
  Bypass Certificate Revocation List (CRL) check
- **chase-referral**  
  Enable chasing referrals from LDAP server
- **crl-check**  
  Enable Certificate Revocation List (CRL) check
- **ldap-agent**  
  LDAP Agent configuration parameters
- **ldap-group-verification**  
  Enable LDAP Group Verification setting
- **ldap-server**  
  LDAP server parameters
- **local**  
  RADIUS local realm
- **nas**  
  RADIUS client
- **no**  
  Negate a command or set its defaults
- **proxy**  
  RADIUS proxy server
- **session-resumption**  
  Enable session resumption/fast reauthentication by using cached attributes
- **termination**  
  Enable EAP termination for proxy requests
- **use**  
  Set setting to use
- **clrscr**  
  Clears the display screen
- **commit**  
  Commit all changes made in this session
- **do**  
  Run commands from Exec mode
- **end**  
  End current mode and change to EXEC mode
- **exit**  
  End current mode and down to previous mode
- **help**  
  Description of the interactive help system
- **revert**  
  Revert changes
- **service**  
  Service Commands
- **show**  
  Show running system information
- **write**  
  Write running configuration to memory or terminal

**Related Commands**

- **no**  
  Removes an existing RADIUS server policy

---

**NOTE:** For more information on RADIUS server policy commands, see **Chapter 16, RADIUS-POLICY**.
4.1.70 radius-user-pool-policy

Global Configuration Commands

Configures a RADIUS user pool

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>

Parameters

- radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>

Examples

rfs7000-37FABE(config)#radius-user-pool-policy testpool
rfs7000-37FABE(config-radius-user-pool-testpool)#?

Radius User Pool Mode commands:

duration Set a guest user’s access duration
no Negate a command or set its defaults
user Radius user configuration

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-user-pool-testpool)#

Related Commands

no Removes an existing RADIUS user pool

NOTE: For more information on RADIUS user group commands, see Chapter 16, RADIUS-POLICY.
4.1.71 rename

Global Configuration Commands

Renames and existing TLO

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

rename tlo <TLO-NAME>

Parameters

- rename tlo <TLO-NAME> <NEW-TLO-NAME>

<table>
<thead>
<tr>
<th>rename tlo &lt;TLO-NAME&gt; &lt;NEW-TLO-NAME&gt;</th>
<th>Renames an existing TLO object</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;TLO-NAME&gt; – Specify the TLO’s name. This is the TLO that is to be renamed.</td>
<td></td>
</tr>
<tr>
<td>• &lt;NEW-TLO-NAME&gt; – Specify the new name for this TLO</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example shows the top level objects available for renaming:

Enter rename and press Tab to list top level objects available for renaming.

```
rename tlo
```

```
rename tlo aaa_policy
rename tlo address_range_alias
rename tlo auto_provisioning_policy
rename tlo bonjour_gw_discovery_policy
rename tlo bonjour_gw_forwarding_policy
rename tlo captive_portal
rename tlo centro_policy
rename tlo client_identity_group
rename tlo crypto_cmp_policy
rename tlo dhcpv6_server_policy
rename tlo evento_system_policy
rename tlo firewall_policy
rename tlo global_assoc_list
rename tlo host_alias
rename tlo ip_acl
rename tlo ipv6_acl
rename tlo ipv6_radv_policy
rename tlo l2tpv3_policy
rename tlo mac_acl
rename tlo management_policy
rename tlo meshpoint_qos
rename tlo mint_policy
rename tlo network_alias
rename tlo network_service_alias
rename tlo profile
rename tlo radio_qos
rename tlo radius_group
rename tlo radius_policy
rename tlo role_policy
rename tlo runtime_license
rename tlo string_alias
rename tlo subscriber_policy
rename tlo url_filter
rename tlo vlan_alias
rename tlo wlan
rename tlo wsm_policy
rename tlo device
```

rfs4000-229D58(config)#
The following examples first clones the existing IP access list **BROADCAST-MULTICAST-CONTROL**, and then renames the cloned IP access list:

```plaintext
rfs4000-229D58(config)#show context
!  ! Configuration of RFS4000 version 5.8.1.0-028D
!  !
!  !
!  !
! client-identity TestClientIdentity
dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!  !
client-identity-group ClientIdentityGroup
client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
  permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
  deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
  deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
  deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
  permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
  permit any any rule-precedence 10 rule-description "permit all IPv4 traffic"
--More--
rfs4000-229D58(config)

rfs4000-229D58(config)#clone ip_acl BROADCAST-MULTICAST-CONTROL TestIP_CLONED
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#show context
!  ! Configuration of RFS4000 version 5.8.1.0-028D
!  !
!  !
! client-identity TestClientIdentity
dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!  !
client-identity-group ClientIdentityGroup
client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
  permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
  deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
  deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
  deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
  permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
ip access-list TestIP_CLONED
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
  permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
--More--
rfs4000-229D58(config)#
```
rfs4000-229D58(config)#rename ip_acl TestIP_CLONED TestIP_RENAMED
rfs4000-229D58(config)#commit

rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.8.1.0-028D
!
!
version 2.1
!
client-identity TestClientIdentity
dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity-group ClientIdentityGroup
  client-identity TestClientIdentity precedence 1
!
ip access-list BROADCAST-MULTICAST-CONTROL
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
  permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
  deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
  deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
  deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
  permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
ip access-list TestIP_RENAMED
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
  permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
--More--
rfs4000-229D58(config)#

**Related Commands**

| **clone** | Creates a replica of an existing TLO or device |
4.1.72 rf-domain

* Global Configuration Commands

An RF Domain groups devices that can logically belong to one network.

The following table lists the RF Domain configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>rf-domain</td>
<td>Creates a RF Domain policy and enters its configuration mode</td>
<td>page 4-298</td>
</tr>
<tr>
<td>rf-domain-mode</td>
<td>Invokes RF Domain configuration mode commands</td>
<td>page 4-300</td>
</tr>
<tr>
<td>commands</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
rf-domain

rf-domain

Creates an RF Domain or enters the RF Domain configuration context for one or more RF Domains. If the RF Domain does not exist, it is created.

The configuration of controllers (wireless controllers, service platforms, and access points) comprises of RF Domains that define regulatory, location, and other relevant policies. At least one default RF Domain is assigned to each controller.

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building, or site. Each RF Domain contains policies that set the Smart RF or WIPS configuration.

RF Domains also enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of access points servicing the global WLAN. This WLAN override eliminates the need to define and manage a large number of individual WLANs and profiles.

A controller’s configuration contains:

- A default RF Domain - Each controller utilizes a default RF Domain. Access Points are assigned to this default RF Domain as they are discovered by the controller. A default RF Domain can be used for single-site and multi-site deployments.
  - Single-site deployment – The default RF Domain can be used for single site deployments, where regional, regulatory, and RF policies are common between devices.
  - Multi-site deployment – A default RF Domain can omit configuration parameters to prohibit regulatory configuration from automatically being inherited by devices as they are discovered. This is desirable in multi-site deployments with devices spanning multiple countries. Omitting specific configuration parameters eliminates the risk of an incorrect country code from being automatically assigned to a device.
- A user-defined RF Domain - Created by administrators. A user-defined RF Domain can be assigned to multiple devices manually or automatically.
  - Manually assigned – Use the CLI or UI to manually assign a user-defined RF Domain to controllers and service platforms.
  - Automatically assigned – Use a AP provisioning policy to automatically assign specific RF Domains to access points based on the access point’s model, serial number, VLAN, DHCP option, and IP address or MAC address. Automatic RF Domain assignments are useful in large deployments, as they enable plug-n-play access point deployments by automatically applying RF Domains to remote access points. For more information on auto provisioning policy, see Chapter 9, AUTO-PROVISIONING-POLICY.

Configure and deploy user-defined RF Domains for single or multiple sites where devices require unique regulatory and regional configurations, or unique Smart RF and WIPS policies. User-defined RF Domains can be used to:

- Assign unique Smart RF or WIPS policies to access points deployed on different floors or buildings within a site.
- Assign unique regional or regulatory configurations to devices deployed in different states or countries.
- Assign unique WLAN SSIDs and/or VLAN IDs to sites assigned a common WLAN without having to define individual WLANs for each site.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600
**Syntax**

```
rf-domain {<RF-DOMAIN-NAME>|containing <RF-DOMAIN-NAME>}
```

**Parameters**

- `rf-domain {<RF-DOMAIN-NAME>|containing <RF-DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>rf-domain</th>
<th>Creates a new RF Domain or enters its configuration context</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RF-DOMAIN-NAME&gt;</code></td>
<td>Optional. Specify the RF Domain name (should not exceed 32 characters and should represent the intended purpose). Once created, the name cannot be edited.</td>
</tr>
<tr>
<td><code>containing &lt;RF-DOMAIN-NAME&gt;</code></td>
<td>Optional. Identifies an existing RF Domain that contains a specified sub-string in the domain name</td>
</tr>
</tbody>
</table>

- `<RF-DOMAIN-NAME>` – Specify a sub-string of the RF Domain name.

**Examples**

```
rfs7000-37FABE(config)#rf-domain rfs7000
rfs7000-37FABE(config-rf-domain-rfs7000)#?
```

**RF Domain Mode commands:**

- `alias` Alias
- `channel-list` Configure channel list to be advertised to wireless clients
- `contact` Configure the contact
- `control-vlan` VLAN for control traffic on this RF Domain
- `controller-managed` RF Domain manager for this domain will be an adopting controller
- `country-code` Configure the country of operation
- `layout` Configure layout
- `location` Configure the location
- `mac-name` Configure MAC address to name mappings
- `no` Negate a command or set its defaults
- `override-smartrf` Configured RF Domain level overrides for smart-rf
- `override-wlan` Configure RF Domain level overrides for wlan
- `sensor-server` AirDefense sensor server configuration
- `stats` Configure the stats related setting
- `timezone` Configure the timezone
- `tree-node` Configure tree node under which this rf-domain appears
- `use` Set setting to use
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-rf-domain-rfs7000)#
```
This section describes the default commands under RF Domain. The following table summarizes RF Domain configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>Configures network, VLAN, and service aliases at the RF Domain level</td>
<td>page 4-301</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures the channel list advertised by radios</td>
<td>page 4-307</td>
</tr>
<tr>
<td>contact</td>
<td>Configures network administrator's contact information (needed in case of any problems impacting the RF Domain)</td>
<td>page 4-308</td>
</tr>
<tr>
<td>control-vlan</td>
<td>Configures VLAN for traffic control on a RF Domain</td>
<td>page 4-309</td>
</tr>
<tr>
<td>controller-managed</td>
<td>Configures the adopting controller or service platform as this RF Domain’s manager</td>
<td>page 4-310</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures the country of operation</td>
<td>page 4-311</td>
</tr>
<tr>
<td>layout</td>
<td>Configures layout information</td>
<td>page 4-312</td>
</tr>
<tr>
<td>location</td>
<td>Configures the physical location of a RF Domain</td>
<td>page 4-314</td>
</tr>
<tr>
<td>mac-name</td>
<td>Maps MAC addresses to names</td>
<td>page 4-315</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts configured settings to their default</td>
<td>page 4-316</td>
</tr>
<tr>
<td>override-smart-rf</td>
<td>Configures RF Domain level overrides for Smart RF</td>
<td>page 4-317</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configures RF Domain level overrides for a WLAN</td>
<td>page 4-318</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server on this RF Domain</td>
<td>page 4-321</td>
</tr>
<tr>
<td>stats</td>
<td>Configures stats related settings on this RF Domain. These settings define how RF Domain statistics are updated.</td>
<td>page 4-323</td>
</tr>
<tr>
<td>timezone</td>
<td>Configures a RF Domain’s geographic time zone</td>
<td>page 4-324</td>
</tr>
<tr>
<td>tree-node</td>
<td>Configures the hierarchical (tree-node) structure under which this RF Domain appears</td>
<td>page 4-325</td>
</tr>
<tr>
<td>use</td>
<td>Enables the use of a specified Smart RF and/or WIPS policy</td>
<td>page 4-327</td>
</tr>
</tbody>
</table>
4.1.72.2.1 alias

rf-domain-mode commands

Configures network, VLAN, host, string, and network-service aliases at the RF Domain level.

This command also allows you to associate existing aliases, created in the global configuration mode, and apply overrides to customize for use at the domain level.

For information on aliases, see alias.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

alias [address-range|host|network|network-group|network-service|number|string|vlan]

alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

alias host <HOST-ALIAS-NAME> <HOST-IP>

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]


alias number <NUMBER-ALIAS-NAME> <0-4294967295>


alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>

Parameters

- address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

<table>
<thead>
<tr>
<th>address-range &lt;ADDRESS-RANGE-ALIAS-NAME&gt;</th>
<th>Creates a new address-range alias for this RF Domain. Or associates an existing address-range alias with this RF Domain. An address-range alias maps a name to a range of IP addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ADDRESS-RANGE-ALIAS-NAME&gt;</td>
<td>Specify the address range alias name.</td>
</tr>
<tr>
<td>Note: Address-range alias name should begin with '$'.</td>
<td></td>
</tr>
<tr>
<td>&lt;STARTING-IP&gt; to &lt;ENDING-IP&gt;</td>
<td>Associates a range of IP addresses with this address range alias</td>
</tr>
<tr>
<td></td>
<td>• &lt;STARTING-IP&gt; — Specify the first IP address in the range.</td>
</tr>
<tr>
<td></td>
<td>• to &lt;ENDING-IP&gt; — Specify the last IP address in the range.</td>
</tr>
<tr>
<td>Note: If using an existing address-range alias, you can apply overrides to the alias at the RF Domain level.</td>
<td></td>
</tr>
</tbody>
</table>
### alias host `<HOST-ALIAS-NAME>` `<HOST-IP>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Creates a host alias for this RF Domain. Or associates an existing host alias with this RF Domain. A host alias maps a name to a single network host.</td>
</tr>
<tr>
<td><code>&lt;HOST-ALIAS-NAME&gt;</code></td>
<td>Specify the host alias name.</td>
</tr>
<tr>
<td><code>&lt;HOST-IP&gt;</code></td>
<td>Associates the network host's IP address with this host alias</td>
</tr>
<tr>
<td><strong>Note:</strong> Alias name should begin with <code>$</code>.</td>
<td></td>
</tr>
</tbody>
</table>

### alias network `<NETWORK-ALIAS-NAME>` `<NETWORK-ADDRESS/MASK>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>Creates a network alias for this RF Domain. Or associates an existing network alias with this RF Domain. A network alias maps a name to a single network address.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-ALIAS-NAME&gt;</code></td>
<td>Specify the network alias name.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-ADDRESS/MASK&gt;</code></td>
<td>Associates a single network with this network alias</td>
</tr>
<tr>
<td><strong>Note:</strong> Alias name should begin with <code>$</code>.</td>
<td></td>
</tr>
</tbody>
</table>

### alias network-group `<NETWORK-GROUP-ALIAS-NAME>` [address-range `<STARTING-IP>` to `<ENDING-IP>`] [host `<HOST-IP>`] [network `<NETWORK-ADDRESS/MASK>`]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-group</td>
<td>Creates a network-group alias for this RF Domain. Or associates an existing network-group alias with this RF Domain.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code></td>
<td>Specify the network-group alias name.</td>
</tr>
<tr>
<td>**Note:**Alias name should begin with <code>$</code>.</td>
<td></td>
</tr>
<tr>
<td>After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If using an existing network-group alias, you can apply overrides to the alias at the RF Domain level.</td>
<td></td>
</tr>
</tbody>
</table>

### address-range `<STARTING-IP>` to `<ENDING-IP>` [address-range `<STARTING-IP>` to `<ENDING-IP>`] [host `<HOST-IP>`] [network `<NETWORK-ADDRESS/MASK>`]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associates a range of IP addresses with this network-group alias</td>
<td></td>
</tr>
<tr>
<td><code>&lt;STARTING-IP&gt;</code></td>
<td>Specify the first IP address in the range.</td>
</tr>
<tr>
<td><code>&lt;ENDING-IP&gt;</code></td>
<td>Specify the last IP address in the range.</td>
</tr>
<tr>
<td><strong>Note:</strong> Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.</td>
<td></td>
</tr>
</tbody>
</table>

### host `<HOST-IP>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associates a single or multiple hosts with this network-group alias</td>
<td></td>
</tr>
<tr>
<td><code>&lt;HOST-IP&gt;</code></td>
<td>Specify the hosts' IP address.</td>
</tr>
<tr>
<td><strong>Note:</strong> Specifies more than one host. A maximum of eight (8) hosts can be configured.</td>
<td></td>
</tr>
</tbody>
</table>

### network `<NETWORK-ADDRESS/MASK>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associates a single or multiple networks with this network-group alias</td>
<td></td>
</tr>
<tr>
<td><code>&lt;NETWORK-ADDRESS/MASK&gt;</code></td>
<td>Specify the network's address and mask.</td>
</tr>
<tr>
<td><strong>Note:</strong> Specifies more than one network. A maximum of eight (8) networks can be configured.</td>
<td></td>
</tr>
</tbody>
</table>
Alias network-service `<NETWORK-SERVICE-ALIAS-NAME>` creates a network-service alias for this RF Domain. Or associates an existing network-service alias with this RF Domain. A network-service alias maps a name to network services and the corresponding source and destination software ports.

- `<NETWORK-SERVICE-ALIAS-NAME>` – Specify a network-service alias name.

**Note:** Alias name should begin with `$`.

**Note:** If using an existing network-service alias, you can apply overrides to the alias at the RF Domain level.

**proto** [0-254]|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp

Use one of the following options to associate an Internet protocol with this network-service alias:

- `<0-254>` – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the **Protocol** field of the IPv4 header and the **Next Header** field of IPv6 header. For example, the **User Datagram Protocol**'s (UDP) designated number is 17.
- `<WORD>` – Identifies the protocol by its name. Specify the protocol name.
- `gre` – Selects Generic Routing Encapsulation (GRE). The protocol number is 47.
- `igmp` – Selects Internet Group Management Protocol (IGMP). The protocol number is 2.
- `ospf` – Selects Open Shortest Path First (OSPF). The protocol number is 89.
- `vrrp` – Selects Virtual Router Redundancy Protocol (VRRP). The protocol number is 112.

**{<1-65535> | <WORD> | bgp|dns|ftp|ftp-data|gopher|https|ldap|ntp|ntp|pop3|proto|sip|smtp|sourceport `<1-65535>` | <WORD> | ssh|telnet|tftp|www})**

After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.

- `<1-65535>` – Optional. Configures a destination port number from 1 - 65535
- `<WORD>` – Optional. Identifies the destination port by the service name provided. For example, the secure shell (SSH) service uses TCP port 22.
- `bgp` – Optional. Configures the default Border Gateway Protocol (BGP) services port (179)
- `dns` – Optional. Configures the default Domain Name System (DNS) services port (53)
- `ftp` – Optional. Configures the default File Transfer Protocol (FTP) control services port (21)
- `ftp-data` – Optional. Configures the default FTP data services port (20)
- `gopher` – Optional. Configures the default gopher services port (70)
- `https` – Optional. Configures the default HTTPS services port (443)
- `ldap` – Optional. Configures the default Lightweight Directory Access Protocol (LDAP) services port (389)
- `ntp` – Optional. Configures the default Newsgroup (NNTP) services port (119)

Contd..
• alias number <NUMBER-ALIAS-NAME> <0-4294967295>

Creates a new number alias or applies an existing number, identified by the <NUMBER-ALIAS-NAME> keyword,
• <NUMBER-ALIAS-NAME> – Specify the number alias name.
• <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.

Note: Number aliases map a name to a numeric value. For example, 'alias number $NUMBER 100'.
• The number alias name is: $NUMBER
• The value assigned is: 100
The value referenced by alias $NUMBER, wherever used, is 100.

• alias string <STRING-ALIAS-NAME> <LINE>

Creates a string alias for this RF Domain. Or associates an existing string alias with this RF Domain. String aliases map a name to an arbitrary string value. For example, alias string $DOMAIN test.example_company.com'. In this example, the string alias name is: $DOMAIN and the string value it is mapped to is: test.example_company.com. In this example, the string alias refers to a domain name.
• <STRING-ALIAS-NAME> – Specify the string alias name.
• <LINE> – Specify the string value.

Note: Alias name should begin with ‘$’.

Note: If using an existing string alias, you can apply overrides to the alias at the RF Domain level.

• alias vlan <VLAN-ALIAS-NAME> <1-4094>

Creates a VLAN alias for this RF Domain. Or associates an existing VLAN alias with this RF Domain. A VLAN alias maps a name to a VLAN ID.
• <VLAN-ALIAS-NAME> – Specify the VLAN alias name.

Note: Alias name should begin with ‘$’.
### Examples

```
rfs4000-229D58(config)#show context
! Configuration of RFS4000 version 5.8.1.0-028D
!
version 2.3
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias network-service $kerberos proto tcp 749 750 80 proto udp 68 sourceport 67
!
alias vlan $TestVLANAlias 1
```

In the following examples, the global aliases `$kerberos` and `$TestVLANAlias` are associated with the RF Domain 'test' and overrides applied:

```
rfs4000-229D58(config-rf-domain-test)#alias network-service $kerberos proto tcp 749 750 80
rfs4000-229D58(config-rf-domain-test)#alias vlan $TestVLANAlias 10
```

Example 1:

In the following examples, the network-group alias `$test` is configured to include hosts 192.168.1.10 and 192.168.1.11, networks 192.168.2.0/24 and 192.168.3.0/24 and address-range 192.168.4.10 to 192.168.4.20.

```
rfs4000-229D58(config)#alias network-group $test host 192.168.1.10 192.168.1.11
rfs4000-229D58(config)#alias network-group $test network 192.168.2.0/24 192.168.3.0/24
rfs4000-229D58(config)#alias network-group $test address-range 192.168.4.10 to 192.168.4.20
```
Associate this network-group alias ‘$test’ to the RF Domain ‘test’ and override the ‘host’ element of the alias.

```
rfs4000-229D58(config-rf-domain-test)#alias network-group $test host 192.168.10.10
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
  no country-code
  alias network-service $kerberos proto tcp 749 750 80
  alias network-group $test host 192.168.10.10
  alias network-group $test network 192.168.2.0/24 192.168.3.0/24
  alias network-group $test address-range 192.168.4.10 to 192.168.4.20
  alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#
```

In the preceding example, the ‘host’ element of the network-group alias ‘$test’ has been overridden. But the ‘network’ and ‘address-range’ elements have been retained as is.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a network, network-group, network-service, VLAN, or string alias from this RF Domain</td>
</tr>
</tbody>
</table>
4.1.72.2.2 channel-list

rf-domain-mode commands

Configures the channel list advertised by radios. This command also enables a dynamic update of a channel list. Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

channel-list [2.4GHz|5GHz|dynamic]

channel-list dynamic

channel-list [2.4GHz|5GHz] <CHANNEL-LIST>

Parameters

- channel-list dynamic

<table>
<thead>
<tr>
<th>dynamic</th>
<th>Enables a dynamic update of a channel list</th>
</tr>
</thead>
</table>

- channel-list [2.4GHz|5GHz] <CHANNEL-LIST>

| 2.4GHz | Configures the channel list advertised by radios operating in the 2.4 GHz mode |
|<CHANNEL-LIST>|  • <CHANNEL-LIST> – Specify the list of channels separated by commas or hyphens. |

| 5GHz | Configures the channel list advertised by radios operating in the 5.0 GHz mode |
|<CHANNEL-LIST>|  • <CHANNEL-LIST> – Specify the list of channels separated by commas or hyphens. |

Examples

rfs7000-37FABE(config-rf-domain-default)#channel-list 2.4GHz 1-10

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
  no country-code
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

no | Removes the list of channels configured on the selected RF Domain for 2.4 GHz and 5.0 GHz bands. Also disables dynamic update of a channel list. |
4.1.72.2.3  contact

rf-domain-mode commands

Configures the network administrator's contact details. The network administrator is responsible for addressing problems impacting the network.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
contact <WORD>

Parameters
- contact <WORD>

Examples
rfs7000-37FABE(config-rf-domain-default)#contact Bob+14082778691
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
  contact Bob+14082778691
  no country-code
  channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs7000-37FABE(config-rf-domain-default)#

Related Commands
- no
  Removes a network administrator’s contact details
4.1.72.2.4 control-vlan

rf-domain-mode commands

Configures the VLAN designated for traffic control in this RF Domain

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
control-vlan <1-4094>

Parameters

- control-vlan <1-4094>

| <1-4094> | Specify the VLAN ID from 1 - 4094. The default is 1. |

Examples
rfs7000-37FABE(config-rf-domain-default)#control-vlan 1

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
no country-code
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

- no
  Disables the VLAN designated for controlling RF Domain traffic
4.1.72.2.5 controller-managed

`rf-domain-mode commands`

Configures the adopting controller (wireless controller, access point, or service platform) as this RF Domain's manager. In other words, the RF Domain is controller managed, and the managing controller is the device managing the RF Domain.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
controller-managed

**Parameters**
None

**Examples**
```
rfs4000-229D58(config-rf-domain-test)#controller-managed
rfs4000-229D58(config-rf-domain-test)#commit
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
  country-code in
  controller-managed
  network-alias techPubs host 192.168.13.8
  network-alias techPubs address-range 192.168.13.10 to 192.168.13.15
  service-alias testing index 10 proto 9 destination-port range 21 21
rfs4000-229D58(config-rf-domain-test)#
```

**Related Commands**
```
no
```
Removes the adopting controller or service platform as this RF Domain’s manager
4.1.72.2.6 country-code

rf-domain-mode commands

Configures a RF Domain’s country of operation. Since device channels transmit in specific channels unique to the country of operation, it is essential to configure the country code correctly or risk using illegal operation.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

country-code <WORD>

Parameters

- country-code <WORD>

<table>
<thead>
<tr>
<th>country-code</th>
<th>Configures the RF Domain’s country of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>Specify the two (2) letter ISO-3166 country code.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-rf-domain-default)#country-code us

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

no

Removes the country of operation configured on a RF Domain
4.1.72.2.7 layout

rf-domain-mode commands

Configures the RF Domain layout in terms of area, floor, and location on a map. It allows users to place APs across the deployment map. A maximum of 256 layouts is permitted.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

layout [area|description|floor|map-location] { (area|description|floor|map-location)}

Parameters

- layout [area <AREA-NAME>|description <LINE>|floor <FLOOR-NAME> {<1-4094>}|map-location <URL> units [feet|meters]}
  - area <AREA-NAME> Configures the RF Domain's layout in terms of the area of location
    - <AREA-NAME> – Specify the area name.
    - Note: After configuring the RF Domain's area of functioning, optionally specify the floor name (and number), description, and/or the location on map.
  - description <LINE> Configures a description for this RF Domain
    - <LINE> – Specify a description that enables you to identify the RF Domain. For a multi-worded string, use double quotes.
  - floor <FLOOR-NAME> <1-4094> Configures the RF Domain's layout in terms of the floor name and number
    - <FLOOR-NAME> – Specify the floor name.
    - <1-4094> – Optional. Specifies the floor number from 1 - 4094. The default floor number is 1.
    - Note: After configuring the RF Domain's floor name (and number), optionally specify the area name, description, and/or the location on map.
  - map-location <URL> units [feet|meters] Configures the location of the RF Domain on the map
    - <URL> – Specify the URL to configure the map location.
    - units [feet|meters] – Configures the map units. The options are: feet or meters
      - feet – Configures the map units in terms of feet
      - meters – Configures the map units in terms of meter
    - Note: After configuring the location of the RF Domain on the map, optionally specify the area name, floor name (and number), and/or description.
Examples
rfs7000-37FABE(config-rf-domain-default)#layout map-location www.firstfloor.com units meters area Ecospace floor Floor1 layout/4.1.

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the RF Domain layout details</td>
</tr>
</tbody>
</table>
4.1.72.2.8 location

rf-domain-mode commands

Configures the RF Domain’s physical location. The location could be as specific as the building name or floor number. Or it could be generic and include an entire site. The location defines the physical area where a set of devices with common configurations are deployed and managed by a RF Domain policy.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

location <WORD>

Parameters

- location <WORD>

Examples

rfs7000-37FABE(config-rf-domain-default)#location SanJose

rfs7000-37FABE(config-rf-domain-default)#show context

rf-domain default
location SanJose
contact Bob+14082778691
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

| no            | Removes the RF Domain location |
4.1.72.2.9 mac-name

rf-domain-mode commands

Configures a relevant name for each MAC address. Use this command to associate client names to specific connected client MAC addresses for improved client management.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
mac-name <MAC> <NAME>

Parameters
- mac-name <MAC> <NAME>

Assigns a user-friendly name to this RF Domain’s member access point’s connected client to assist in its easy recognition
- <MAC> – Specify the MAC address
- <NAME> – Specify the client name for the specified MAC address. The name specified here will be used in events and statistics.

Examples
rfs7000-37FABE(config-rf-domain-default)#mac-name 11-22-33-44-55-66 TestDevice

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
location SanJose
contact Bob+14082778691
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
mac-name 11-22-33-44-55-66 TestDevice
layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#

Related Commands
no

Removes the MAC address to name mapping
4.1.7.2.2.10 no

- **rf-domain-mode commands**

Negates a command or reverts configured settings to their default. When used in the config RF Domain mode, the *no* command negates or reverts RF Domain settings.

**Supported in the following platforms:**

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`no [alias|channel-list|contact|control-vlan|controller-managed|country-code|layout|location|mac-name|override-smartrf|override-wlan|sensor-server|stats|timezone|tree-node|use]`

**Parameters**

- `no <PARAMETERS>`

`no <PARAMETERS>` Removes or reverts this RF Domain’s settings based on the parameters passed

**Examples**

The following example shows the default RF Domain settings before the ‘no’ commands are executed:

```
no channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
no mac-name 11-22-33-44-55-66 TestDevice
```

The following example shows the default RF Domain settings after the ‘no’ commands are executed:

```
no channel-list 2.4GHz 1-10
no mac-name 11-22-33-44-55-66
no location
no control-vlan
```
4.72.2.11 override-smart-rf

rf-domain-mode commands

Enables dynamic channel switching for Smart RF radios. This command allows you to configure an override list of channels that Smart RF can use for channel compensations on 2.4 GHz and 5.0 GHz radios.

When a radio fails or is faulty, a Smart RF policy provides automatic recovery by instructing neighboring access points to increase their transmit power to compensate for the coverage loss. Once correct access point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events and can ensure availability of adequate detector coverage.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
override-smart-rf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

Parameters

- **override-smart-rf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>override-smart-rf</strong></td>
<td>Enables dynamic channel switching for Smart RF radios</td>
</tr>
<tr>
<td><strong>channel-list</strong></td>
<td>Configures a list of channels for 2.4 GHz and 5.0 GHz Smart RF radios</td>
</tr>
<tr>
<td><strong>2.4GHz &lt;CHANNEL-LIST&gt;</strong></td>
<td>Selects the 2.4 GHz Smart RF radio channels</td>
</tr>
<tr>
<td></td>
<td>- <strong>&lt;CHANNEL-LIST&gt;</strong> – Specify a list of channels separated by commas.</td>
</tr>
<tr>
<td><strong>5GHz &lt;CHANNEL-LIST&gt;</strong></td>
<td>Selects the 5.0 GHz Smart RF radio channels</td>
</tr>
<tr>
<td></td>
<td>- <strong>&lt;CHANNEL-LIST&gt;</strong> – Specify a list of channels separated by commas.</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-rf-domain-default)#override-smart-rf channel-list 2.4GHz 1,2,3
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
country-code us
layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
rfs7000-37FABE(config-rf-domain-default)#
```

Related Commands

- **no** Removes the override-smart-rf list of channels configured for 2.4 GHz and 5.0 GHz radios
### 4.1.72.2.12 override-wlan

**rf-domain-mode commands**

Configures RF Domain level overrides for a WLAN

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
overrides-wlan <WLAN-NAME> [shutdown|ssid|vlan-pool|wep128|wpa-wpa2-psk]  
overrides-wlan <WLAN-NAME> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192}>]  
  wpa-wpa2-psk <PASSPHRASE>]  
overrides-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]  
overrides-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|  
  transmit-key <1-4>]  
```

#### Parameters

- **overrides-wlan <WLAN-NAME> [shutdown|ssid|vlan-pool|wep128|wpa-wpa2-psk]**
  - `<WLAN-NAME>` Configures the WLAN name
    - If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN’s coverage area. After creating the WLAN, configure its override parameters.
  - **shutdown** Shuts down WLAN operation on all mapped radios
  - **ssid <SSID>** Configures a override SSID associated with this WLAN
    - `<SSID>` – Specify the SSID (should not exceed 32 characters in length).
    - Each WLAN provides associated wireless clients with a SSID. This has limitations, because it requires wireless clients to associate with different SSIDs to obtain QoS and security policies. However, a WiNG-managed RF Domain can have WLANs assigned and advertise a single SSID, and yet allow users to inherit different QoS or security policies.
  - **vlan-pool <1-4094> {limit <0-8192}>**
    - Configures the override VLANs available to this WLAN
      - `<1-4094>` – Specify the VLAN ID from 1 - 4094.
      - `<limit <0-8192>>` – Optional. Sets a limit to the number of users on this VLAN from 0 - 8192. The default is 0.
    - Controllers and service platforms allow the mapping of a WLAN to more than one VLAN. Wireless clients associating with a WLAN are assigned VLANs, from the pool representative of the WLAN, in a way that ensures proper load balancing across VLANs. Clients are tracked per VLAN, and assigned to the least used/loaded VLAN. Client VLAN usage is tracked on a per-WLAN basis. The maximum allowed client limit is 8192 per VLAN.
### overrides-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]

| <WLAN-NAME> | Configures the WLAN name  
If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN’s coverage area. After creating the WLAN, configure its override parameters. |
| wpa-wpa2-psk | Overrides a WLAN’s existing WPA-WPA2 pre-shared key or passphrase at the RF Domain level. WPA2 is a newer 802.11i standard that provides wireless security that is stronger than Wi-Fi Protected Access (WPA) and WEP.  
• <PASSPHRASE> – Specify a WPA-WPA2 key or passphrase. It is an alphanumeric string of 8 to 64 ASCII characters or 64 HEX characters as the primary string, which both the transmitting and receiving authenticators must share in this new override PSK. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the you the necessity of entering the 256-bit key each time keys are generated. |

### overrides-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|transmit-key <1-4>]

| <WLAN-NAME> | Configures the WLAN name  
If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN’s coverage area. After creating the WLAN, configure its override parameters. |
| wep128 | Overrides a WLAN’s existing WEP128 keys at the RF Domain level (not the profile level). WEP128 uses a 104 bit key, which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data on the WLAN. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.  
| key <1-4> hex | Configures the WEP128 key.  
A total of four keys can be configured.  
• <1-4> – Select the key index from 1- 4.  
• hex – Configures a hexadecimal key  
  • 0 <WORD> – Configures a clear text key  
  • 2 <WORD> – Configures an encrypted key  
The following parameter is common to both clear-text and encrypted key options:  
• <WORD> – Specify the WEP128/Keyguard key (should not exceed 26 hexadecimal characters in length). |
| transmit-key | Configures transmit WEP/Keyguard key settings  
• <1-4> – Transmit the key identified by the key index specified here. Specify the index from 1 - 4. |
Examples
rfs7000-37FABE(config-rf-domain-default)#override-wlan test vlan-pool 2 limit 20
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
  contact Bob+14082778691
  country-code us
  override-smartrf channel-list 2.4GHz 1,2,3
  override-wlan test vlan-pool 2 limit 20
  layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the override WLAN settings its default</td>
</tr>
</tbody>
</table>
4.1.72.2.13 sensor-server

rf-domain-mode commands

Configures an AirDefense sensor server on this RF Domain. Sensor servers allow network administrators to monitor and download data from multiple sensors remote locations using Ethernet TCP/IP or serial communications. This enables administrators to respond quickly to interferences and coverage problems. The **Wireless Intrusion Protection System** (WIPS) protects the controller managed network, wireless clients and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the controller). Unique WIPS server configurations can be used by RF Domains to ensure a WIPS server configuration is available to support the unique data protection needs of individual RF Domains.

WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the access point radio(s) available to each controller managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz bands. Sensor support requires a AirDefense WIPS Server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
sensor-server <1-3> ip <IP> {port [443|<1-65535>]}
```

Parameters

- **sensor-server <1-3> ip <IP> {port [443|<1-65535>]}**

<table>
<thead>
<tr>
<th>sensor-server</th>
<th>Configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3&gt;</td>
<td>Configures an AirDefense sensor server parameters</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-3&gt; – Select the server ID from 1 - 3. The server with the lowest defined ID is reached first. The default is 1.</td>
</tr>
<tr>
<td>ip &lt;IP&gt;</td>
<td>Configures the (non DNS) IPv4 address of the sensor server</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP&gt; – Specify the IPv4 address of the sensor server.</td>
</tr>
<tr>
<td>port [443</td>
<td>&lt;1-65535&gt;]</td>
</tr>
<tr>
<td></td>
<td>• 443 – Configures port 443, the default port used by the AirDefense server</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Allows you to select a WIPS/AirDefense sensor server port from 1 - 65535</td>
</tr>
</tbody>
</table>
Examples

```
rf7000-37FABE(config-rf-domain-default)#sensor-server 2 ip 172.16.10.3 port 443

rf7000-37FABE(config-rf-domain-default)#show context
rf-domain default
  contact Bob+14082778691
  country-code us
  sensor-server 2 ip 172.16.10.3
  override-smartrf channel-list 2.4GHz 1,2,3
  override-wlan test vlan-pool 2 limit 20
  layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
rf7000-37FABE(config-rf-domain-default)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables an AirDefense sensor server parameters</td>
</tr>
</tbody>
</table>
4.1.72.2.14 stats

*rf-domain-mode commands*

Configures stats settings that define how RF Domain statistics are updated

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
stats update-interval
```
```
stats update-interval [<5-300>|auto]
```

**Parameters**
```
• stats update-interval [<5-300>|auto]
```

| stats update-interval [<5-300>|auto] | Configures the interval at which RF Domain statistics are updated. The options are:
|--------------------------------------|--------------------------------------------------|
| <5-300> | Specify an update interval from 5 - 300 seconds.
| auto | The RF Domain manager automatically adjusts the update interval based on the load.

**Examples**
```
rfs7000-37FABE(config-rf-domain-default)#stats update-interval 200
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
stats update-interval 200
country-code us
sensor-server 2 ip 172.16.10.3
override-smartrf channel-list 2.4GHz 1,2,3
override-wlan test vlan-pool 2 limit 20
layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
rfs7000-37FABE(config-rf-domain-default)#
```

**Related Commands**
```
no | Resets stats related settings
```

4.1.72.2.15 timezone

rf-domain-mode commands

Configures the RF Domain’s geographic time zone. By default all WiNG devices are shipped with the time zone and time format set to Universal Time Coordinated (UTC) and 24-hour clock respectively. If the time zone is not reset, all devices within the RF Domain will display time relative to the UTC - Greenwich Time. Resetting the time zone is recommended, especially for RF Domains deployed across different geographical locations. The time zone can either be set on a specific device or on an RF Domain. When configured as RF Domain setting, it applies to all devices within the domain. For more information on configuring the time zone on a device, see timezone.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
timezone <TIMEZONE>
```

Parameters

- timezone <TIMEZONE>

Examples

```
$ rfs7000-37FABE(config-rf-domain-default)#timezone America/Los_Angeles

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
    contact Bob+14082778691
timezone America/Los_Angeles
stats update-interval 200
country-code us
sensor-server 2 ip 172.16.10.3
override-smartrf channel-list 2.4GHz 1,2,3
override-wlan test vlan-pool 2 limit 20
layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
rfs7000-37FABE(config-rf-domain-default)#
```

The built-in WiNG timezones are:

```
nx9500-6C8809(config-rf-domain-test)#timezone <TAB>
Africa/  Asia/  Atlantic/  Australia/  CET  CST6CDT
EET  EST5EDT  Etc/  Europe/  MST7MDT  Pacific/
PST8PDT  US/  America/
nx9500-6C8809(config-rf-domain-test)#
```

Each of these time zones are further differentiated into sub time zones. For example, as shown in the following example:

```
nx9500-6C8809(config-rf-domain-test)#timezone Africa/
Africa/Cairo  Africa/Casablanca  Africa/Harare
Africa/Johannesburg  Africa/Lagos  Africa/Nairobi
nx9500-6C8809(config-rf-domain-test)#
```

Related Commands

- **no** Removes a RF Domain’s time zone
4.1.72.2.16 tree-node

rf-domain-mode commands

Configures the hierarchical (tree-node) structure under which this RF Domain is located.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

tree-node [campus|city|country|region] {(campus|city|country|region)}

Parameters

- tree-node [campus|city|country|region] {(campus|city|country|region)}

Usage Guidelines

- Adding a country first is a good idea since region, city, and campus can all be added as sub-nodes in the tree structure. However, the selected country is an invalid tree node until a RF Domain is mapped.
- A city and campus can be added in the tree structure as sub-nodes under a region. An RF Domain can be placed anywhere down the hierarchy for a region and not just directly under a country. For example, a region can have city, campus, and one RF Domain mapped.
- Only a campus can be added as a sub-node under a city. The city is an invalid tree node until a RF Domain is mapped somewhere within the directory tree.
- A campus is the last node in the hierarchy before a RF Domain, and it is not valid unless it has a RF Domain mapped.
- After creating the tree structure do a commit and save for the tree configuration to take effect and persist across reboots.

Note: At least one of these four nodes must be defined. This feature is disabled by default.
Examples

```
rfs4000-229D58(config-rf-domain-test)#tree-node campus EcoSpace City Bangalore
country India region South
rfs4000-229D58(config-rf-domain-test)#

rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
country-code in
tree-node country India region South city Bangalore campus EcoSpace
rfs4000-229D58(config-rf-domain-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the RF Domain's tree-node configuration</td>
</tr>
</tbody>
</table>
4.1.72.2.17 use

rf-domain-mode commands

Enables the use of Smart RF and WIPS with this RF Domain

Assigns an existing Wireless IPS (WIPS) policy to the RF Domain

A WIPS policy provides protection against wireless threats and acts as a key layer of security complementing wireless VPNs, encryption and authentication. A WIPS policy uses a dedicated sensor for actively detecting and locating rogue AP devices. After detection, WIPS uses mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

use [license|nsight-policy|smart-rf-policy|wips-policy]

use [license <WEB-FILTERING-LICENSE>|nsight-policy <POLICY-NAME>|smart-rf-policy <SMART-RF-POLICY-NAME>|wips-policy <WIPS-POLICY-NAME>]

Parameters

- use [license <LICENSE>|nsight-policy <POLICY-NAME>|smart-rf-policy <SMART-RF-POLICY-NAME>|wips-policy <WIPS-POLICY-NAME>]

<table>
<thead>
<tr>
<th>use</th>
<th>Uses a Smart RF policy with this RF Domain</th>
</tr>
</thead>
</table>
| license <WEB-FILTERING-LICENSE> | Obtains the specified Web filtering license from the adopting controller
  - <WEB-FILTERING-LICENSE> – Specify the WEBF license name. |
| nsight-policy <POLICY-NAME> | Applies an NSight policy to this RF Domain
  - <POLICY-NAME> – Specify the NSight policy name (Should be existing and configured). When applied, it enables the RF Domain manager to gather statistical data from access points within the domain and forward to the NOC running the NSight server. |
| smart-rf-policy <SMART-RF-POLICY-NAME> | Specifies a Smart RF policy
  - <SMART-RF-POLICY-NAME> – Specify the Smart RF policy name. For more information on configuring smart RF policy, see SMART-RF-POLICY. |
| wips-policy <WIPS-POLICY-NAME> | Specifies a WIPS policy
  - <WIPS-POLICY-NAME> – Specify the WIPS policy name. For more information on configuring WIPS policy, see WIPS-POLICY. |
Examples

rfs7000-37FABE(config-rf-domain-default)#use smart-rf-policy Smart-RF1
rfs7000-37FABE(config-rf-domain-default)#use wips-policy WIPS1
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
  contact Bob+14082778691
timezone America/Los_Angeles
stats update-interval 200
country-code us
  use smart-rf-policy Smart-RF1
  use wips-policy WIPS1
sensor-server 2 ip 172.16.10.3
override-smartrf channel-list 2.4GHz 1,2,3
override-wlan test vlan-pool 2 limit 20
layout area Ecospace floor Floor5 map-location www.firstfloor.com units meters
rfs7000-37FABE(config-rf-domain-default)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets profiles used with this RF Domain</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server on this RF Domain</td>
</tr>
<tr>
<td>wips-policy</td>
<td>Configures a WIPS policy</td>
</tr>
<tr>
<td>smart-rf-policy</td>
<td>Configures a Smart RF policy</td>
</tr>
</tbody>
</table>
4.1.73 rfs4000

Global Configuration Commands

Adds an RFS4000 wireless controller to the network

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

rfs4000 <DEVICE-RFS4000-MAC>

Parameters

- rfs4000 <DEVICE-RFS4000-MAC>

| <DEVICE-RFS4000-MAC> | Specify the RFS4000’s MAC address. |

Examples

rfs7000-37FABE(config)#rfs4000 10-20-30-40-50-60
rfs7000-37FABE(config-device-10-20-30-40-50-60)#

Related Commands

- no
  Removes an RFS4000 wireless controller from the network
4.1.74 **rfs6000**

*Global Configuration Commands*

Adds a RFS6000 wireless controller to the network

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
rfs6000 <DEVICE-RFS6000-MAC>
```

**Parameters**

- `rfs6000 <DEVICE-RFS6000-MAC>`

**Examples**

```
rfs7000-37FABE(config)#rfs6000 11-20-30-40-50-61
rfs7000-37FABE(config-device-11-20-30-40-50-61)#
```

**Related Commands**

- `no` Removes a RFS6000 wireless controller from the network
4.1.75 rfs7000

Global Configuration Commands

Adds a RFS7000 wireless controller to the network

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

rfs7000 <DEVICE-RFS7000-MAC>

Parameters

- rfs7000 <DEVICE-RFS7000-MAC>

<table>
<thead>
<tr>
<th>&lt;DEVICE-RFS7000-MAC&gt;</th>
<th>Specify the RFS7000's MAC address.</th>
</tr>
</thead>
</table>

Examples

rfs7000-37FABE(config)#rfs7000 12-20-30-40-50-62
rfs7000-37FABE(config-device-12-20-30-40-50-62)#

Related Commands

| no | Removes a RFS7000 wireless controller from the network |
4.1.76 **nx45xx**

*Global Configuration Commands*

Adds an integrated NX45XX series service platform to the network. If a profile for service platform is not available, a new profile is created.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

---

**NOTE:** In this guide, NX4500 and NX4524 are collectively represented as a NX45XX series service platform.

---

**Syntax**

nx45xx <DEVICE-NX45XX-MAC>

**Parameters**

- nx45xx <DEVICE-NX45XX-MAC>

<table>
<thead>
<tr>
<th>&lt;DEVICE-NX45XX-MAC&gt;</th>
<th>Specifies the MAC address of a NX45XX series service platform.</th>
</tr>
</thead>
</table>

**Examples**

nx9500-6C8809(config)#nx45xx B4-C7-99-5C-FA-8E
nx9500-6C8809(config-device-B4-C7-99-5C-FA-8E)#

**Related Commands**

- *no* Removes a NX45XX series service platform from the network
4.1.77 nx5500

Global Configuration Commands

Adds an integrated NX5500 series service platform to the network. If a profile for this service platform is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

nx5500 <DEVICE-NX5500-MAC>

Parameters

- nx5500 <DEVICE-NX5500-MAC>

<table>
<thead>
<tr>
<th>&lt;DEVICE-NX5500-MAC&gt;</th>
<th>Specifies the MAC address of a NX5500 series service platform.</th>
</tr>
</thead>
</table>

Examples

nx9500-6C8809(config)#nx5500 B4-C7-02-3C-FA-6E
nx9500-6C8809(config-device-B4-C7-02-3C-FA-6E)#

Related Commands

- **no** | Removes a NX5500 series service platform from the network |
4.1.78 nx65xx

Global Configuration Commands

Adds an integrated NX65XX series service platform to the network. If a profile for service platform is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

nx65xx <DEVICE-NX65XX-MAC>

Parameters

- nx65xx <DEVICE-NX65XX-MAC>

Examples

```
nx9500-6C8809(config)#nx65xx 00-15-70-88-9E-C4
nx9500-6C8809(config-device-00-15-70-88-9E-C4)#
```

Related Commands

- no

Removes a NX65XX series service platform from the network

NOTE: In this guide, NX6500 and NX6524 are collectively represented as a NX65XX series service platform.
4.1.79 nx75xx

Global Configuration Commands

Adds an integrated NX75XX series service platform to the network. If a profile for service platform is not available, a new profile is created.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

nx75xx <DEVICE-NX75XX-MAC>

Parameters

- nx75xx <DEVICE-NX75XX-MAC>

Examples

nx9500-6C8809(config)#nx75xx B4-C9-81-6C-FA-7C
nx9500-6C8809(config-device-B4-C9-81-6C-FA-7C)#show context

```
x75xx B4-C9-81-6C-FA-7C
  use profile default-nx75xx
  use rf-domain default
  hostname nx75xx-6CFA7C
nx9500-6C8809(config-device-B4-C9-81-6C-FA-7C)#
```

nx75xx-6CFA7C>show adoption status
Adopted by:
  Type : nx9000
  System Name : nx9500-6C8809
  MAC address : B4-C7-99-6C-88-09
  MiNT address : 19.6C.88.09
  Time : 1 days 01:57:50 ago

Adopted Devices:

```
DEVICE-NAME VERSION    CFG-STAT   MSGS ADOPTED-BY               LAST-ADOPTION    UPTIME
ap7131-11B6C4 5.8.1.0-021D configured No  nx75xx-6CFA7C 1 days 01:49:44 1 days 01:59:34
```

Total number of devices displayed: 1

nx75xx-6CFA7C>

Related Commands

- no | Removes a NX75XX series service platform from the network
4.1.80 nx9000

Global Configuration Commands

Adds a NX9000 series service platform to the network

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
nx9000 <DEVICE-NX9000-MAC>
```

Parameters

- `nx9000 <DEVICE-NX9000-MAC>`

Examples

```
nx9500-6C8809(config)#nx9000 B4-C7-89-7C-81-08
nx9500-6C8809(config-device-B4-C7-89-7C-81-08)#
```

Related Commands

- `no` Removes a NX9000 series service platform from the network

 NOTE: In this guide, NX9000, NX9500, and NX9510 are collectively represented as a NX9000 series service platform.
4.1.81 Roaming-Assist-Policy

Global Configuration Commands

Configures a roaming assist policy that enables access points to assist wireless clients in making roaming decisions, such as which access point to connect etc.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

roaming-assist-policy <POLICY-NAME>

Parameters

- roaming-assist-policy <POLICY-NAME>

Examples

rfs7000-37FABE(config)#roaming-assist-policy testPolicy
rfs7000-37FABE(config-roaming-assist-policy-testPolicy)#?

Roaming Assist Mode commands:

- action: Configure action - action is either to log / deauth client
- aggressiveness: Configure the roaming aggressiveness for a wireless client
- detection-threshold: Configure the detection threshold - when exceeded, client monitoring starts
- disassoc-time: Configure the disassociation time - time after which a disassociation is sent
- handoff-count: Configure the handoff count - number of times client can exceed handoff threshold
- handoff-threshold: Configure the handoff threshold - when exceeds an action is taken.
- monitoring-interval: Configure the monitoring interval - interval at which client monitoring occurs
- no: Negate a command or set its defaults
- sampling-interval: Configure the sampling interval - interval at which client rssi values are checked
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

rfs7000-37FABE(config-roaming-assist-policy-testPolicy)#

**NOTE:** For more information on roaming assist policy commands, see Chapter 30, ROAMING ASSIST POLICY.

Related Commands

- no: Removes an existing roaming assist policy
### 4.1.82 role-policy

**Global Configuration Commands**

Configures a role-based firewall policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

role-policy <ROLE-POLICY-NAME>

**Parameters**

- role-policy <ROLE-POLICY-NAME>

**Examples**

rfs7000-37FABE(config)#role-policy role1
rfs7000-37FABE(config-role-policy-role1)#?

Role Policy Mode commands:

- default-role  Configuration for Wireless Clients not matching any role
- ldap-deadperiod  Ldap dead period interval
- ldap-query  Set the ldap query mode
- ldap-server  Add a ldap server
- ldap-timeout  Ldap query timeout interval
- no  Negate a command or set its defaults
- user-role  Create a role
- clrscr  Clears the display screen
- commit  Commit all changes made in this session
- do  Run commands from Exec mode
- end  End current mode and change to EXEC mode
- exit  End current mode and down to previous mode
- help  Description of the interactive help system
- revert  Revert changes
- service  Service Commands
- show  Show running system information
- write  Write running configuration to memory or terminal

rfs7000-37FABE(config-role-policy-role1)#

---

**NOTE:** For more information on role policy commands, see Chapter 18, ROLE-POLICY.

---

**Related Commands**

- **no**  Removes an existing role policy
4.1.83 route-map

*Global Configuration Commands*

Creates a dynamic BGP route map and enters its configuration mode

BGP route maps are used by network administrators to define rules controlling redistribution of routes between routers and routing processes. These route maps are also used to control and modify routing information.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

route-map <ROUTE-MAP-NAME>

**Parameters**

- route-map <ROUTE-MAP-NAME>

**Examples**

nx9500-6C8809(config)#route-map test

nx9500-6C8809(config-dr-route-map-test)#?

Route Map Mode commands:
- deny     Add a deny route map rule to deny set operations
- no       Negate a command or set its defaults
- permit   Add a permit route map rule to permit set operations
- clrscr   Clears the display screen
- commit   Commit all changes made in this session
- do       Run commands from Exec mode
- end      End current mode and change to EXEC mode
- exit     End current mode and down to previous mode
- help     Description of the interactive help system
- revert   Revert changes
- service  Service Commands
- show     Show running system information
- write    Write running configuration to memory or terminal

nx9500-6C8809(config-dr-route-map-test)#

**Related Commands**

- no          Removes an existing dynamic BGP route map

**NOTE:** For more information on BGP route maps, see *Chapter 28, BORDER GATEWAY PROTOCOL.*
### 4.1.84 `routing-policy`

**Global Configuration Commands**

Configures a routing policy

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
routing-policy <ROUTING-POLICY-NAME>
```

**Parameters**

- `routing-policy <ROUTING-POLICY-NAME>`

**Examples**

```
rfs7000-37FABE(config)#routing-policy TestRoutingPolicy
rfs7000-37FABE(config-routing-policy-TestRoutingPolicy)#?
```

Routing Policy Mode commands:

- `apply-to-local-packets` Use Policy Based Routing for packets generated by the device
- `logging` Enable logging for this Route Map
- `no` Negate a command or set its defaults
- `route-map` Create a Route Map
- `use` Set setting to use
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-routing-policy-TestRoutingPolicy)#
```

**NOTE:** For more information on routing policy commands, see Chapter 24, `ROUTING-POLICY`.

**Related Commands**

- `no` Removes an existing routing policy
4.1.85 self

Displays the logged device's configuration context

Supported in the following platforms:
  • Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  • Wireless Controllers — RFS4000, RFS6000, RFS7000
  • Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

self

Parameters

None

Examples

rfs7000-37FABE(config)#self
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
### 4.1.86 smart-rf-policy

**Global Configuration Commands**

Configures a Smart RF policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

smart-rf-policy <SMART-RF-POLICY-NAME>

#### Parameters

- smart-rf-policy <SMART-RF-POLICY-NAME>

<table>
<thead>
<tr>
<th>&lt;SMART-RF-POLICY-NAME&gt;</th>
<th>Specify the Smart RF policy name. If the policy does not exist, it is created.</th>
</tr>
</thead>
</table>

#### Examples

rfs7000-37FABE(config)#smart-rf-policy test
rfs7000-37FABE(config-smart-rf-policy-test)#?

Smart RF Mode commands:

- area
  - Specify channel list/ power for an area
- assignable-power
  - Specify the assignable power during power-assignment
- avoidance-time
  - Time to avoid a channel once dfs/adaptivity avoidance is necessary
- channel-list
  - Select channel list for smart-rf
- channel-width
  - Select channel width for smart-rf
- coverage-hole-recovery
  - Recover from coverage hole
- enable
  - Enable this smart-rf policy
- group-by
  - Configure grouping parameters
- interference-recovery
  - Recover issues due to excessive noise and interference
- neighbor-recovery
  - Recover issues due to faulty neighbor radios
- no
  - Negate a command or set its defaults
- sensitivity
  - Configure smart-rf sensitivity (Modifies various other smart-rf configuration items)
- smart-ocs-monitoring
  - Smart off channel scanning
- clrscr
  - Clears the display screen
- commit
  - Commit all changes made in this session
- end
  - End current mode and change to EXEC mode
- exit
  - End current mode and down to previous mode
- help
  - Description of the interactive help system
- revert
  - Revert changes
- service
  - Service Commands
- show
  - Show running system information
- write
  - Write running configuration to memory or term

rfs7000-37FABE(config-smart-rf-policy-test)#

---

**NOTE:** For more information on Smart RF policy commands, see *Chapter 19, SMART-RF-POLICY.*

---

**Related Commands**

| no | Removes an existing Smart RF policy |
4.1.87 t5

Global Configuration Commands

Invokes the configuration mode of a t5 wireless controller

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5’s management within a WiNG supported subnet populated by both types of devices.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

t5 <T5-DEVICE-MAC>

Parameters

- t5 <T5-DEVICE-MAC>

<table>
<thead>
<tr>
<th>t5 &lt;T5-DEVICE-MAC&gt;</th>
<th>Specify the t5 device’s MAC address. The system enters the identified device's configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5’s management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the IPX operating system. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE’s physical wallplate connection and phone jack. Note: After logging on to the T5 device, use the ‘cpe’ keyword and configure the following mandatory settings:</td>
</tr>
<tr>
<td></td>
<td>• vlan – Set a VLAN from 1 - 4,094 used as a virtual interface for connections between the T5 controller and its managed CPE devices.</td>
</tr>
<tr>
<td></td>
<td>• start ip – Set a starting IP address used in a range of addresses available to T5 controller connecting CPE devices.</td>
</tr>
<tr>
<td></td>
<td>• end ip – Set an end IP address used in a range of addresses available to T5 controller connecting CPE devices.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config)#t5 B4:C7:99:ED:5C:2C
rfs7000-37FABE(config-device-B4:C7:99:ED:5C:2C)#?

T5 Device Mode commands:

- adsp-sensor-server Configure WIPS server
- bridge Sets MAC address expiration time in the bridge address table
- clock Configure clock options
- cpe T5 CPE configuration
- hostname Set system’s network name
- interface Select an interface to configure
- ip Internet Protocol (IP)
- no Negate a command or set its defaults
- ntp Configure NTP
- override-wlan Configure RF Domain level overrides for wlan
- password T5 password configuration
- qos QoS settings
- radius-server Radius server settings
- t5 T5 configuration
- t5-logging Modify message logging facilities
use                  Set setting to use
clrscr               Clears the display screen
commit               Commit all changes made in this session
do                   Run commands from Exec mode
end                   End current mode and change to EXEC mode
exit                  End current mode and down to previous mode
help                  Description of the interactive help system
revert               Revert changes
service               Service Commands
show                  Show running system information
write                 Write running configuration to memory or terminal

rfs7000-37FABE(config-device-B4:C7:99:ED:5C:2C)#

Related Commands

| no                  | Removes the t5 wireless controller identified by the device’s MAC address |
### 4.1.88 web-filter-policy

The following table lists commands that enable you to enter the Web Filter policy configuration mode:

**Table 4.37 Commands Creating a Web-Filter-Policy**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-filter-policy</td>
<td>Creates a new Web Filter policy and enters its configuration mode</td>
<td>page 4-468</td>
</tr>
<tr>
<td>web-filter-policy-config-mode commands</td>
<td>Summarizes the Web Filter policy configuration mode commands</td>
<td>page 4-347</td>
</tr>
</tbody>
</table>
4.1.88.1 web-filter-policy

web-filter-policy

Creates a Web Filtering policy and enters its configuration mode. This policy defines rules managing the local classification database and the cached data. When configured and applied, this policy also enables caching of URL classification records in a local database in a controller-based, hierarchically managed (HM) deployment. Use this option to specify the following: classification server details, size of the local database, time for which records are cached in the database, the action taken in case the classification server is unavailable etc.

The Web filter policy is applied at the profile or device level.

For more information on URL filtering, see url-filter.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

web-filter-policy <WEB-FILTER-POLICY-NAME>

Parameters

- web-filter-policy <WEB-FILTER-POLICY-NAME>

Examples

nx4500-5CFA2B(config)#web-filter-policy test
nx4500-5CFA2B(config-web-filter-policy-test)#?

Content Filter Mode commands:
- cache-max-recs Configure the maximum number of records in local cache
- cache-save-interval Configure the time a record is saved in local cache
- logging Select logging method
- no Negate a command or set its defaults
- server-host Configure URL classification server if it is not the adopted controller
- server-unreachable Permission to access website when classification server is unreachable (default is pass)
- uncategorized-url Permission to website when server fails to classify the URL request (default is pass)
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

nx4500-5CFA2B(config-web-filter-policy-test)#

Related Commands

- no Removes an existing Web filter policy
4.1.88.2 web-filter-policy-config-mode commands

The following table summarizes Web Filter policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache-max-recs</td>
<td>Configures the maximum number of records (URLs and Web pages) cached in the local database</td>
<td>page 4-348</td>
</tr>
<tr>
<td>cache-save-interval</td>
<td>Configures the maximum time period for which a record (URL and Web page classification entry) is cached in the local database</td>
<td>page 4-349</td>
</tr>
<tr>
<td>logging</td>
<td>Configures the method used to log Web filtering events</td>
<td>page 4-350</td>
</tr>
<tr>
<td>no</td>
<td>Reverts the selected Web Filter policy settings to default</td>
<td>page 4-351</td>
</tr>
<tr>
<td>server-host</td>
<td>Configures the URL classification server in case it is not the adopted controller</td>
<td>page 4-352</td>
</tr>
<tr>
<td>server-unreachable</td>
<td>Configures the action taken in case the classification server is unreachable</td>
<td>page 4-353</td>
</tr>
<tr>
<td>uncategorized-url</td>
<td>Configures the action taken in case the classification server fails to classify a URL/Website</td>
<td>page 4-354</td>
</tr>
</tbody>
</table>
4.1.88.2.1 cache-max-recs

This command configures the maximum number of records (URL and Web page classification entries) cached in the local database.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

`cache-max-recs <1-100000>`

Parameters

- `cache-max-recs <1-100000>`

Specify the maximum number of records cached in the local database from 1 - 100000. When configuring this value take into consideration the type of device using the Web Filter policy. The value should approximately be as per the following information:

- NX95XX – <1-100000> (default is 100,000)
- NX45XX/NX65XX/NX75XX – <1-100000> (default is 10,000)
- RFS Switches – <1-10000> (default is 1,000)
- Access Points – <1-1500> (default is 500)

Examples

```
nx4500-5CFA2B(config-web-filter-policy-test)#cache-max-recs 9000
```

```
nx4500-5CFA2B(config-web-filter-policy-test)#show context web-filter-policy test
cache-max-recs 9000
```

Related Commands

`no`

Reverts the maximum number of stored records to default. Please see the parameter table for default values for the different device types.
4.1.88.2.2 cache-save-interval

Configure the maximum time period, in seconds, for which a record (URL and Web page classification entry) is cached in the local database. Once the specified time has expired the record is removed from the cache.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

\texttt{cache-save-interval <1-86400>}

Parameters

- \texttt{cache-save-interval <1-86400>}

| cache-save-interval \texttt{<1-86400>} | Specify the maximum time period, in seconds, for which a record is cached in the local database from 1 - 86400 seconds. The default is 60 seconds. |

Examples

\begin{verbatim}
nx4500-5CFA2B(config-web-filter-policy-test)#cache-save-interval 1000

nx4500-5CFA2B(config-web-filter-policy-test)#show context
web-filter-policy test
  cache-max-recs 9000
  cache-save-interval 1000

nx4500-5CFA2B(config-web-filter-policy-test)#
\end{verbatim}

Related Commands

| no | Reverts the maximum time period for which a record (URL and Web page classification entry) is cached in the local database to default (60) |
4.1.88.2.3 logging

web-filter-policy-config-mode commands

Configures the method used to log Web filtering events

Supported in the following platforms:

• Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

logging [logfile|syslog]

Parameters

• logging [logfile|syslog]

| logging [logfile|syslog] | Selects the method used to log Web filtering events. The options are:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• logfile – Logs to a file.</td>
</tr>
<tr>
<td></td>
<td>• syslog – Logs to the syslog server. This is the default setting.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-web-filter-policy-test)#logging logfile

nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
logging logfile
nx9500-6C8809(config-web-filter-policy-test)#
no

web-filter-policy-config-mode commands

Reverts the selected Web Filter policy settings to default, based on the parameters passed.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

no [cache-max-recs|cache-save-interval|server-host|server-unreachable|uncategorized-url]

Parameters
- no <PARAMETERS>

Examples

The following example shows the Web Filter policy 'test' settings before the 'no' command is executed:


nx4500-5CFA2B(config-web-filter-policy-test)#no cache-max-recs
nx4500-5CFA2B(config-web-filter-policy-test)#no server-unreachable
nx4500-5CFA2B(config-web-filter-policy-test)#no uncategorized-url

The following example shows the Web Filter policy 'test' settings after the 'no' command has been executed:


nx4500-5CFA2B(config-web-filter-policy-test)#
4.1.88.2.5 server-host

Configures the URL classification server in case it is not the adopted controller

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
server-host [host-name <SERVER-HOST-NAME>|ip-address <SERVER-IPv4>|
imint-id <SERVER-MiNT-ID>]
```

Parameters

- `server-host [host-name <SERVER-HOST-NAME>|ip-address <SERVER-IPv4>|
imint-id <SERVER-MiNT-ID>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-name</td>
<td>Identifies the classification server by its hostname.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Identifies the classification server by its IP address.</td>
</tr>
<tr>
<td>mint-id</td>
<td>Identifies the classification server by its MiNT ID.</td>
</tr>
</tbody>
</table>

Examples

```
nx4500-5CFA2B(config-web-filter-policy-test)#server-host ip-address 192.168.13.13

nx4500-5CFA2B(config-web-filter-policy-test)#show context
web-filter-policy test
  cache-max-recs 9000
  cache-save-interval 1000
  server-host ip-address 192.168.13.13

nx4500-5CFA2B(config-web-filter-policy-test)#
```

Related Commands

- `no` Removes the URL classification server's configured details, such as hostname, ip-address, or MiNT ID.
4.1.88.2.6 server-unreachable

web-filter-policy-config-mode commands

Configures the action taken in case the classification server is unreachable. Based on the value configured the an end user’s request for a URL/Website is either blocked or passed.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

server-unreachable [block|pass]

Parameters

- server-unreachable [block|pass]

| server-unreachable [block|pass] | Configures the action taken in case the classification server is unreachable. The options are:
| | • block – Denies access to the requested URL/Website
| | • pass – Allows access to the requested URL/Website. This is the default value. |

Examples

nx4500-5CFA2B(config-web-filter-policy-test)#server-unreachable block

nx4500-5CFA2B(config-web-filter-policy-test)#show context
web-filter-policy test
  cache-max-recs 9000
  cache-save-interval 1000
  server-unreachable block
  server-host ip-address 192.168.13.13
nx4500-5CFA2B(config-web-filter-policy-test)#

Related Commands

- no | Reverts the action taken in case the classification server is unreachable to default (pass)
### 4.1.88.2.7 uncategorized-url

**web-filter-policy-config-mode commands**

Configures the action taken in case the classification server fails to classify a URL/Website. Based on the value configured the an end user’s request for a non-classified URL/Website is either blocked or passed.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
uncategorized-url [block|pass]
```

**Parameters**

- `uncategorized-url [block|pass]`

  **Examples**

  - `nx4500-5CFA2B(config-web-filter-policy-test)#uncategorized-url block`
  - `nx4500-5CFA2B(config-web-filter-policy-test)#show context`
  - `web-filter-policy test`
  - `cache-max-recs 9000`
  - `cache-save-interval 1000`
  - `uncategorized-url block`
  - `server-unreachable block`
  - `server-host ip-address 192.168.13.13`
  - `nx4500-5CFA2B(config-web-filter-policy-test)#`

**Related Commands**

- `no`

  Reverts the action taken in case the classification server fails to classify a URL/Website to default (pass)
4.1.89 **wips-policy**

> **Global Configuration Commands**

Configures a WIPS policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wips-policy <WIPS-POLICY-NAME>
```

**Parameters**

- `wips-policy <WIPS-POLICY-NAME>`

**Examples**

```
rfs7000-37FABE(config)#wips-policy test
rfs7000-37FABE(config-wips-policy-test)#?
```

Wips Policy Mode commands:

- `ap-detection` Rogue AP detection
- `enable` Enable this wips policy
- `event` Configure an event
- `history-throttle-duration` Configure the duration for which event duplicates are not stored in history
- `interference-event` Specify events which will contribute to smart-rf wifi interference calculations
- `no` Negate a command or set its defaults
- `signature` Signature to configure
- `use` Set setting to use

```
clrscr
commit
end
exit
help
revert
service
show
write
```

```
rfs7000-37FABE(config-wips-policy-test)#
```

---

**NOTE:** For more information on WIPS policy commands, see *Chapter 20, WIPS-POLICY.*

---

**Related Commands**

- `no` Removes an existing WIPS policy
4.1.90 wlan

Global Configuration Commands

Configures a Wireless Local Area Network (WLAN)

The following table lists WLAN configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>Creates a new wireless LAN and enters its configuration mode</td>
<td>page 4-357</td>
</tr>
<tr>
<td>wlan-mode commands</td>
<td>Summarizes WLAN configuration mode commands</td>
<td>page 4-360</td>
</tr>
</tbody>
</table>
4.1.90.1 **wlan**

Configures a WLAN and enters its configuration mode. Use this command to modify an existing WLAN’s settings. A WLAN is a data-communications system that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or Orthogonal Frequency Division Multiplexing (OFDM) modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), e-mail, file, and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHZ radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHZ and 5.0 GHZ radios at the branch site to provide complete coverage.

The maximum number of WLANs supported by different devices is as follows:

- RFS4000 and RFS6000 wireless controllers – 32 WLANs
- RFS7000 wireless controller – 256 WLANs
- NX4500 and NX6500 series service platforms – 32 WLANs
- NX9000 series service platforms – 1000 WLANs
- Access Points – 16 WLANs

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

**Parameters**

- wlan {<WLAN-NAME>|containing <WLAN-NAME>}

  - wlan `<WLAN-NAME>` Configures a new WLAN
    - `<WLAN-NAME>` – Optional. Specify the WLAN name.
    - The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing etc.). The name cannot exceed 32 characters.

  - containing `<WLAN-NAME>` Optional. Configures an existing WLAN’s settings
    - `<WLAN-NAME>` – Specify a sub-string in the WLAN name. Use this parameter to filter a WLAN. This option allows you to select and enter the configuration mode of one or more WLANs.
### Examples

```bash
rfs7000-37FABE(config)#wlan 1
rfs7000-37FABE(config-wlan-1)#?
```

Wireless LAN Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Configure how accounting records are created for this wlan</td>
</tr>
<tr>
<td>acl</td>
<td>Actions taken based on ACL configuration [packet drop being one of them]</td>
</tr>
<tr>
<td>answer-broadcast-probes</td>
<td>Include this wlan when responding to probe requests that do not specify an SSID</td>
</tr>
<tr>
<td>assoc-response</td>
<td>Association response threshold</td>
</tr>
<tr>
<td>association-list</td>
<td>Configure the association list for the wlan</td>
</tr>
<tr>
<td>authentication-type</td>
<td>The authentication type of this WLAN</td>
</tr>
<tr>
<td>bridging-mode</td>
<td>Configure how packets to/from this wlan are bridged</td>
</tr>
<tr>
<td>broadcast-dhcp</td>
<td>Configure broadcast DHCP packet handling</td>
</tr>
<tr>
<td>broadcast-ssid</td>
<td>Advertise the SSID of the WLAN in beacons</td>
</tr>
<tr>
<td>captive-portal-enforcement</td>
<td>Enable captive-portal enforcement on the wlan</td>
</tr>
<tr>
<td>client-access</td>
<td>Enable client-access (normal data operations) on this wlan</td>
</tr>
<tr>
<td>client-client-communication</td>
<td>Allow switching of frames from one wireless client to another on this wlan</td>
</tr>
<tr>
<td>client-load-balancing</td>
<td>Configure load balancing of clients on this wlan</td>
</tr>
<tr>
<td>controller-assisted-mobility</td>
<td>Enable controller assisted mobility to determine wireless clients' VLAN assignment</td>
</tr>
<tr>
<td>data-rates</td>
<td>Specify the 802.11 rates to be supported on this wlan</td>
</tr>
<tr>
<td>description</td>
<td>Configure a description of the usage of this wlan</td>
</tr>
<tr>
<td>downstream-group-addressed-forwarding</td>
<td>Enable downstream group addressed forwarding of packets</td>
</tr>
<tr>
<td>dynamic-vlan-assignment</td>
<td>Dynamic VLAN assignment configuration</td>
</tr>
<tr>
<td>eap-types</td>
<td>Configure client access based on eap-type used for authentication</td>
</tr>
<tr>
<td>encryption-type</td>
<td>Configure the encryption to use on this wlan</td>
</tr>
<tr>
<td>enforce-dhcp</td>
<td>Drop packets from Wireless Clients with static IP address</td>
</tr>
<tr>
<td>fast-bss-transition</td>
<td>Configure support for 802.11r Fast BSS Transition</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enable HTTP URL analysis on the wlan</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>ipv6</td>
<td>Internet Protocol version 6 (IPv6)</td>
</tr>
<tr>
<td>kerberos</td>
<td>Configure kerberos authentication parameters</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>Configure mac-authentication related parameters</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>opendns</td>
<td>OpenDNS related config for this wlan</td>
</tr>
<tr>
<td>protected-mgmt-frames</td>
<td>Protected Management Frames (IEEE 802.11w) related configuration (DEMO FEATURE)</td>
</tr>
<tr>
<td>proxy-arp-mode</td>
<td>Configure handling of ARP requests with proxy-arp is enabled</td>
</tr>
<tr>
<td>proxy-nd-mode</td>
<td>Configure handling of IPv6 ND requests with proxy-nd is enabled</td>
</tr>
<tr>
<td>qos-map</td>
<td>Support the 802.11u QoS map element and frame</td>
</tr>
<tr>
<td>radio-resource-measurement</td>
<td>Configure support for 802.11k Radio Resource Measurement</td>
</tr>
</tbody>
</table>
radius                                 Configure RADIUS related parameters
registration                           Enable dynamic registration of device
(or) user                              (or) user
relay-agent                             Configure dhcp relay agent info
shutdown                               Shutdown this wlan
ssid                                    Configure the Service Set Identifier
for this WLAN
*t5-client-isolation                   Isolate traffic among clients
*t5-security                           Configure encryption and
authentication
*time-based-access                     Configure client access based on time
use                                     Set setting to use
vlan                                    Configure the vlan where traffic from
this wlan is mapped
vlan-pool-member                       Add a member vlan to the pool of
vlans for the wlan (Note: configuration of a vlan-pool
overrides the 'vlan' configuration)
wep128                                  Configure WEP128 parameters
wep64                                   Configure WEP64 parameters
*wing-extensions                       Enable support for WiNG-Specific
extensions to 802.11
wireless-client                        Configure wireless-client specific
parameters
wpa-wpa2                               Modify tkip-ccmp (wpa/wpa2) related
parameters
clrscr                                 Clears the display screen
commit                                  Commit all changes made in this
session
do                                      Run commands from Exec mode
end                                      End current mode and change to EXEC
mode
exit                                    End current mode and down to previous
mode
help                                    Description of the interactive help
system
revert                                  Revert changes
service                                 Service Commands
show                                    Show running system information
write                                   Write running configuration to memory
or terminal

rfs7000-37FABE(config-wlan-1)#

The following example shows how to use the ‘containing’ keyword to enter the configuration mode of an existing WLAN:

rfs7000-37FABE(config)#wlan containing wlan1
rfs7000-37FABE(config-wlan-{'containing': 'wlan1'})#
4.1.90.2 wlan-mode commands

This section documents the WLAN configuration mode commands in detail.
Use the (config) instance to configure WLAN related parameters.
To navigate to this instance, use the following command:

```
<DEVICE>(config)#wlan <WLAN-NAME>
```

The following table summarizes WLAN configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Defines a WLAN accounting configuration</td>
<td>page 4-363</td>
</tr>
<tr>
<td>acl</td>
<td>Defines the actions based on an ACL rule configuration</td>
<td>page 4-365</td>
</tr>
<tr>
<td>answer-broadcast-probes</td>
<td>Allows a WLAN to respond to probes for broadcast ESS</td>
<td>page 4-367</td>
</tr>
<tr>
<td>assoc-response</td>
<td>Configures a minimum receive signal strength indication (RSSI) value, below which the WLAN does not send a response to a client's association request</td>
<td>page 4-368</td>
</tr>
<tr>
<td>association-list</td>
<td>Attaches an existing global association list to a WLAN</td>
<td>page 4-369</td>
</tr>
<tr>
<td>authentication-type</td>
<td>Sets a WLAN's authentication type</td>
<td>page 4-370</td>
</tr>
<tr>
<td>bridging-mode</td>
<td>Configures how packets to/from this WLAN are bridged</td>
<td>page 4-372</td>
</tr>
<tr>
<td>broadcast-dhcp</td>
<td>Configures broadcast DHCP packet handling</td>
<td>page 4-373</td>
</tr>
<tr>
<td>broadcast-ssid</td>
<td>Advertises a WLAN’s SSID in beacons</td>
<td>page 4-374</td>
</tr>
<tr>
<td>captive-portal-enforcement</td>
<td>Configures a WLAN’s captive portal enforcement</td>
<td>page 4-375</td>
</tr>
<tr>
<td>client-access</td>
<td>Enables WLAN client access (normal data operations)</td>
<td>page 4-376</td>
</tr>
<tr>
<td>client-client-communication</td>
<td>Allows the switching of frames from one wireless client to another on a WLAN</td>
<td>page 4-377</td>
</tr>
<tr>
<td>client-load-balancing</td>
<td>Enables load balancing of WLAN clients</td>
<td>page 4-378</td>
</tr>
<tr>
<td>controller-assisted-mobility</td>
<td>Enables controller assisted mobility to determine wireless clients' VLAN assignment</td>
<td>page 4-380</td>
</tr>
<tr>
<td>data-rates</td>
<td>Specifies the 802.11 rates supported on the WLAN</td>
<td>page 4-381</td>
</tr>
<tr>
<td>description</td>
<td>Sets a WLAN’s description</td>
<td>page 4-384</td>
</tr>
<tr>
<td>downstream-group-addressed-forwarding</td>
<td>Enables forwarding of downstream packets addressed to a group</td>
<td>page 4-385</td>
</tr>
<tr>
<td>dynamic-vlan-assignment</td>
<td>Configures dynamic VLAN assignment on this WLAN</td>
<td>page 4-386</td>
</tr>
<tr>
<td>eap-types</td>
<td>Configures client access based on eap-type used for authentication</td>
<td>page 4-387</td>
</tr>
</tbody>
</table>
### Table 4.40 WLAN-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption-type</td>
<td>Sets a WLAN's encryption type</td>
<td>page 4-389</td>
</tr>
<tr>
<td>enforce-dhcp</td>
<td>Drops packets from clients with a static IP address</td>
<td>page 4-390</td>
</tr>
<tr>
<td>fast-bss-transition</td>
<td>Configures support for 802.11r fast BSS transition on a WLAN</td>
<td>page 4-391</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enables HTTP URL analysis on the WLAN</td>
<td>page 4-392</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IPv4 settings on this WLAN</td>
<td>page 4-394</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures IPv6 settings on this WLAN</td>
<td>page 4-395</td>
</tr>
<tr>
<td>kerberos</td>
<td>Configures Kerberos authentication parameters</td>
<td>page 4-396</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>Configures MAC authentication parameters</td>
<td>page 4-398</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 4-399</td>
</tr>
<tr>
<td>opendns</td>
<td>Configures the device ID, which is embedded in each DNS query packet going out from an access point, wireless controller, or service platform to the OpenDNS server</td>
<td>page 4-403</td>
</tr>
<tr>
<td>protected-mgmt-frames</td>
<td>Enables and configures the WLAN's frame protection mode and security association</td>
<td>page 4-406</td>
</tr>
<tr>
<td>proxy-arp-mode</td>
<td>Enables the proxy ARP mode for ARP requests</td>
<td>page 4-408</td>
</tr>
<tr>
<td>proxy-nd-mode</td>
<td>Configures the proxy ND mode for this WLAN member clients as either strict or dynamic</td>
<td>page 4-409</td>
</tr>
<tr>
<td>qos-map</td>
<td>Enables support for 802.11u QoS map element and frames</td>
<td>page 4-410</td>
</tr>
<tr>
<td>radio-resource-measurement</td>
<td>Enables support for 802.11k radio resource measurement</td>
<td>page 4-411</td>
</tr>
<tr>
<td>radius</td>
<td>Configures RADIUS parameters</td>
<td>page 4-412</td>
</tr>
<tr>
<td>registration</td>
<td>Configures settings enabling dynamic registration of devices. Use this command to specify the mode of registration and to configure corresponding parameters.</td>
<td>page 4-414</td>
</tr>
<tr>
<td>relay-agent</td>
<td>Enables support for DHCP relay agent information (option 82) feature on this WLAN</td>
<td>page 4-416</td>
</tr>
<tr>
<td>shutdown</td>
<td>Auto shuts down a WLAN</td>
<td>page 4-418</td>
</tr>
<tr>
<td>ssid</td>
<td>Configures a WLAN's SSID</td>
<td>page 4-420</td>
</tr>
<tr>
<td>t5-client-isolation</td>
<td>Disallows clients connecting to the WLAN to communicate with one another</td>
<td>page 4-421</td>
</tr>
<tr>
<td>t5-security</td>
<td>Configures T5 PowerBroadband security settings</td>
<td>page 4-422</td>
</tr>
<tr>
<td>time-based-access</td>
<td>Configures time-based client access</td>
<td>page 4-424</td>
</tr>
<tr>
<td>use</td>
<td>Defines WLAN mode configuration settings</td>
<td>page 4-425</td>
</tr>
<tr>
<td>vlan</td>
<td>Sets VLAN assignment for a WLAN</td>
<td>page 4-428</td>
</tr>
</tbody>
</table>
### Table 4.40 WLAN-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-pool-member</code></td>
<td>Adds a member VLAN to the pool of VLANs for a WLAN</td>
<td>page 4-429</td>
</tr>
<tr>
<td><code>wep128</code></td>
<td>Configures WEP128 parameters</td>
<td>page 4-431</td>
</tr>
<tr>
<td><code>wep64</code></td>
<td>Configures WEP64 parameters</td>
<td>page 4-433</td>
</tr>
<tr>
<td><code>wing-extensions</code></td>
<td>Enables support for WiNG specific extensions to 802.11</td>
<td>page 4-435</td>
</tr>
<tr>
<td><code>wireless-client</code></td>
<td>Configures the transmit power for wireless clients transmission</td>
<td>page 4-437</td>
</tr>
<tr>
<td><code>wpa-wpa2</code></td>
<td>Modifies TKIP and CCMP (WPA/WPA2) related parameters</td>
<td>page 4-440</td>
</tr>
<tr>
<td><code>service</code></td>
<td>Invokes service commands applicable in the WLAN configuration mode</td>
<td>page 4-443</td>
</tr>
</tbody>
</table>
4.1.90.2.1 accounting

Defines the WLAN’s accounting configuration

Accounting is the method of collecting user data, such as start and stop times, executed commands (for example, PPP), number of packets and number of bytes received and transmitted. This data is sent to the security server for billing, auditing, and reporting purposes. Accounting enables wireless network administrators to track the services and network resources accessed and consumed by users. When enabled, this feature allows the network access server to report and log user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA policies.

Accounting can be enabled and applied to access point, wireless controller, or service platform managed WLANs. Once enabled, it uniquely logs accounting events specific to the managed WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to a location outside of the access point for periodic network and user permission administration.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
accounting [radius|syslog|wait-client-ip]
accounting [radius|wait-client-ip]
accounting syslog [host|mac-address-format]
accounting syslog host <IP/HOSTNAME> {port <1-65535>}{proxy-mode [none|through-controller|through-rf-domain-manager]}
accounting syslog mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot] case [lower|upper]
```

Parameters

- accounting [radius|wait-client-ip]

| accounting radius | Enables support for WLAN RADIUS accounting messages. This option is disabled by default. When enabled, the WLAN uses an external RADIUS resource for accounting. Note: Use the use > aaa-policy > <AAA-POLICY-NAME> command to associate an appropriate AAA policy with this WLAN. This AAA policy should be existing and should define the accounting, authentication, and authorization parameters. |
| accounting wait-client-ip | Enables waiting for client’s IP before commencing the accounting procedure |

- accounting syslog host <IP/HOSTNAME> {port <1-65535>}{proxy-mode [none|through-controller|through-rf-domain-manager]}

<p>| accounting syslog | Enables support for WLAN syslog accounting messages in standard syslog format (RFC 3164). This option is disabled by default. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Configures a syslog destination hostname or IP address for accounting records</td>
</tr>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Specify the IP address or name of the destination host.</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Configures the syslog server’s UDP port (this port is used to connect to the server)</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Specify the port from 1 - 65535. Default port is 514.</td>
</tr>
<tr>
<td>proxy-mode [none</td>
<td>through-controller</td>
</tr>
<tr>
<td></td>
<td>• none – Requests are directly sent to the server from the device</td>
</tr>
<tr>
<td></td>
<td>• through-controller – Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device</td>
</tr>
<tr>
<td></td>
<td>• through-rf-domain-manager – Proxies requests through the local RF Domain manager</td>
</tr>
<tr>
<td>accounting syslog</td>
<td>Enables support for WLAN syslog accounting messages</td>
</tr>
<tr>
<td>mac-address-format</td>
<td>Configures the MAC address format used in syslog messages</td>
</tr>
<tr>
<td>middle-hyphen</td>
<td>Configures the MAC address format with middle hyphen (AABBCC-DDEEFF)</td>
</tr>
<tr>
<td>no-delim</td>
<td>Configures the MAC address format without delimiters (AABBCCDDEEFF)</td>
</tr>
<tr>
<td>pair-colon</td>
<td>Configures the MAC address format with pair-colon delimiters (AA:BB:CC:DD:EE:FF)</td>
</tr>
<tr>
<td>pair-hyphen</td>
<td>Configures the MAC address format with pair-hyphen delimiters (AA-BB-CC-DD-EE-FF). This is the default setting.</td>
</tr>
<tr>
<td>quad-dot</td>
<td>Configures the MAC address format with quad-dot delimiters (AABB.CCDD.EEFF)</td>
</tr>
<tr>
<td>case [lower</td>
<td>upper]</td>
</tr>
<tr>
<td></td>
<td>• case – Specifies MAC address case (upper or lower)</td>
</tr>
<tr>
<td></td>
<td>• lower – Specifies MAC address is filled in lower case (for example, aa-bb-cc-dd-ee-ff)</td>
</tr>
<tr>
<td></td>
<td>• upper – Specifies MAC address is filled in upper case (for example, AA-BB-CC-DD-EE-FF)</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-wlan-test)#accounting syslog host 172.16.10.4 port 2 proxy-mode none
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  accounting syslog host 172.16.10.4 port 2
rfs7000-37FABE(config-wlan-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables sending of accounting message to the RADIUS server, disables syslog accounting, or disables waiting for client’s IP before sending accounting messages</td>
</tr>
</tbody>
</table>
4.1.90.2.2 acl

Defines the actions taken based on an ACL rule configuration

Use the `use > ip-access-list <IP-ACCESS-LIST-NAME>` command to associate an ACL with the WLAN. The ACL rule is determined by the associated ACL's configuration.

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms allowing and denying data traffic in respect to administrator defined rules. For an overview of firewalls, see `FIREWALL-POLICY`.

WLANs use firewalls like Access Control Lists (ACLs) to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of Access Control Entries (ACEs). Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
_acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>|disassociate}
```

Parameters

- `acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>|disassociate}`

<table>
<thead>
<tr>
<th>acl exceed-rate</th>
<th>Sets the action taken based on an ACL rule configuration (for example, drop a packet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless-client-denied-traffic &lt;0-1000000&gt;</td>
<td>Sets the action to deny traffic to the wireless client when the rate exceeds the specified value</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-1000000&gt; — Specify a allowed rate threshold of disallowed traffic in packets/sec.</td>
</tr>
<tr>
<td></td>
<td>• If enabled, this option allows an associated client, exceeding the thresholds configured for storm traffic, to be either de-authenticated or blacklisted depending on the action selected. This option is disabled by default.</td>
</tr>
<tr>
<td>blacklist &lt;0-86400&gt;</td>
<td>Optional. When enabled, sets the time interval, in seconds, to blacklist a wireless client.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-86400&gt; — Configures the blacklist duration from 0 - 86400 seconds. Offending clients are re-authenticated once the blacklist duration, configured here, has exceeded.</td>
</tr>
<tr>
<td>disassociate</td>
<td>Optional. When enabled, disassociates a wireless client.</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-wlan-test)#acl exceed-rate wireless-client-denied-traffic 20 disassociate

rfs7000-37FABE(config-wlan-test)#show context wlan test
    ssid test
    bridging-mode tunnel
    encryption-type none
    authentication-type none
    accounting syslog host 172.16.10.4 port 2
    acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs7000-37FABE(config-wlan-test) #

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the action (de-authenticate or blacklist) to be taken when an associated client exceeds the thresholds configured for storm traffic</td>
</tr>
</tbody>
</table>
4.1.90.2.3 answer-broadcast-probes

Allows the WLAN to respond to probe requests that do not specify a SSID. These probes are for broadcast ESS. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
answer-broadcast-probes

Parameters
None

Examples
rfs7000-37FABE(config-wlan-1)#answer-broadcast-probes
rfs7000-37FABE(config-wlan-1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Does not allow this WLAN to respond to probe requests that do not specify a SSID</td>
</tr>
</tbody>
</table>
4.1.90.2.4 assoc-response

wlan-mode commands

Configures the deny-threshold and rssi-threshold values. These threshold values are considered when responding to a client’s association/authentication request.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
assoc-response [deny-threshold <1-12>|rssi-threshold <-100--40>]

Parameters
- assoc-response [deny-threshold <1-12>|rssi-threshold <-100--40>]

<table>
<thead>
<tr>
<th>assoc-response</th>
<th>Configures the association response thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny-threshold &lt;1-12&gt;</td>
<td>Configures the number of times association/authentication request, from a client, is ignored if the RSSI is less than the configured RSSI threshold. This option is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-12&gt; – Specify the deny-threshold from 1 - 12.</td>
</tr>
<tr>
<td>rssi-threshold &lt;-100--40&gt;</td>
<td>Configures an association response RSSI threshold value. If the RSSI is below the configured threshold value, the client’s association/authentication request is ignored. This option is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• rssi-threshold &lt;-100--40&gt; – Specify a value from -100 - -40 dBm.</td>
</tr>
</tbody>
</table>

Examples
nx9500-6C8809(config-wlan-test)#assoc-response rssi-threshold -60
nx9500-6C8809(config-wlan-test)#assoc-response deny-threshold 4

nx9500-6C8809(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode local
  encryption-type none
  authentication-type none
  assoc-response rssi-threshold -60
  assoc-response deny-threshold 4
  registration user group-name guest expiry-time 2000 agreement-refresh 14400

nx9500-6C8809(config-wlan-test)#

Related Commands

no | Removes the configured deny-threshold and rssi-threshold values |
### 4.1.90.2.5 association-list

*Wlan-mode commands*

Attaches an existing global association list with this WLAN. For more information on global association lists, see `global-association-list`.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

**Parameters**
- `association-list global <GLOBAL-ASSO-LIST-NAME>`

**Examples**

```
rfs4000-229D58(config-wlan-test)#association-list global my-clients
rfs4000-229D58(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  association-list global my-clients
rfs4000-229D58(config-wlan-test)#
```

**Related Commands**

```
no
```

Removes the global association list's association with this WLAN.
### 4.1.90.2.6 authentication-type

* wlan-mode commands

Sets the WLAN's authentication type

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```

#### Parameters

- `authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]`

<table>
<thead>
<tr>
<th>authentication-type</th>
<th>Configures a WLAN's authentication type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The authentication types are: EAP, EAP-MAC, EAP-PSK, Kerberos, MAC, and none.</td>
</tr>
</tbody>
</table>

- `eap`

  Configures EAP authentication (802.1X)

  EAP is the de-facto standard authentication method used to provide secure authenticated access to controller managed WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over controller managed WLANs.

  The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client’s identity.

  If using EAP authentication ensure that a AAA policy is mapped to the WLAN.

- `eap-mac`

  Configures EAP or MAC authentication depending on client. (This setting is valid only with the None encryption type.

  EAP-MAC is useful when in a hotspot environment, as some clients support EAP and an administrator may want to authenticate based on just the MAC address of the device.

- `eap-psk`

  Configures EAP authentication or pre-shared keys depending on client. (This setting is only valid with Temporal Key Integrity Protocol (TKIP) or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption types.

  When using PSK with EAP, the controller sends a packet requesting a secure link using a pre-shared key. The controller and authenticating device must use the same authenticating algorithm and pass code during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP.

  If using eap-psk authentication ensure that a AAA policy is mapped to the WLAN.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos</td>
<td>Configures Kerberos authentication (encryption will change to WEP128 if it’s not already WEP128 or Keyguard) &lt;br&gt;Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection. Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with 802.11b clients. Kerberos uses Network Time Protocol (NTP) for synchronizing the clocks of its Key Distribution Center (KDC) server(s).</td>
</tr>
<tr>
<td>mac</td>
<td>Configures MAC authentication (RADIUS lookup of MAC address) &lt;br&gt;MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP. MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date restrictions. MAC authentication can only identify devices, not users. If using mac authentication ensure that a AAA policy is mapped to the WLAN.</td>
</tr>
<tr>
<td>none</td>
<td>No authentication is used or the client uses pre-shared keys. This is the default value.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-wlan-test)#authentication-type eap
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type eap
  accounting syslog host 172.16.10.4 port 2
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs7000-37FABE(config-wlan-test)#
```

**Related Commands**

- **no** | Resets the authentication mode used with this WLAN to default (none/pre-shared keys) |
4.1.90.2.7 bridging-mode

wlan-mode commands

Configures how packets are bridged to and from a WLAN

Use this command to define which VLANs are bridged, and how local VLANs are bridged between the wired and wireless sides of the network.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

bridging-mode [local|tunnel]

Parameters

- bridging-mode [local|tunnel]

<table>
<thead>
<tr>
<th>bridging-mode</th>
<th>Configures how packets are bridged to and from a WLAN. The options are local and tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Bridges packets between WLAN and local ethernet ports. This is the default mode.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Tunnels packets to other devices (typically a wireless controller or service platform)</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-wlan-test)#bridging-mode local

rfs7000-37FABE(config-wlan-test)#show context wlan test
ssid test
  bridging-mode local
  encryption-type none
  authentication-type eap
  accounting syslog host 172.16.10.4 port 2
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
rfs7000-37FABE(config-wlan-test)#
4.1.90.2.8 broadcast-dhcp

- **wlan-mode commands**

Configures broadcast DHCP packet handling parameters

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

broadcast-dhcp validate-offer

**Parameters**

- broadcast-dhcp validate-offer

<table>
<thead>
<tr>
<th>validate-offer</th>
<th>Enables validation of the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air. This option is disabled by default.</th>
</tr>
</thead>
</table>

**Examples**

rfs7000-37FABE(config-wlan-test)#broadcast-dhcp validate-offer

rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode local
  encryption-type none
  authentication-type eap
  accounting syslog host 172.16.10.4 port 2
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
  broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#

**Related Commands**

- no | Disables validation of the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air |
4.1.90.2.9 broadcast-ssid

Advertises the WLAN SSID in beacons. If a hacker tries to isolate and hack a SSID from a client, the SSID will display since the ESSID is in the beacon. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX5600, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
broadcast-ssid

Parameters
None

Examples
rfs7000-37FABE(config-wlan-1)#broadcast-ssid
rfs7000-37FABE(config-wlan-1)#

Related Commands

|   no   | Disables the broadcasting of the WLAN’s SSID in beacons |
**4.1.90.2.10 captive-portal-enforcement**

- wlan-mode commands

Configures the WLAN’s captive portal enforcement

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
captive-portal-enforcement {fall-back}

**Parameters**
- captive-portal-enforcement {fall-back}

<table>
<thead>
<tr>
<th>captive-portal-enforcement</th>
<th>Enables captive portal enforcement on a WLAN. This option is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>fall-back</td>
<td>Optional. Enforces captive portal validation if WLAN authentication fails (applicable to EAP or MAC authentication only)</td>
</tr>
</tbody>
</table>

**Examples**
rfs7000-37FABE(config-wlan-test)#captive-portal-enforcement fall-back
rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
 rfs7000-37FABE(config-wlan-test)#

**Related Commands**

| no | Disables captive portal enforcement |
4.1.90.2.11 client-access

* wlan-mode commands

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

client-access

Parameters

None

Examples

rfs7000-37FABE(config-wlan-1)#client-access
rfs7000-37FABE(config-wlan-1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Enables WLAN client access</td>
</tr>
</tbody>
</table>
4.1.90.2.12 client-client-communication

wlan-mode commands

Allows frame switching from one client to another on a WLAN

This option is enabled by default. It allows clients to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is also disabled on that WLAN, clients are not permitted to interoperate.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

client-client-communication

Parameters

None

Examples

rfs7000-37FABE(config-wlan-1)#client-client-communication
rfs7000-37FABE(config-wlan-1)#

Related Commands

no Disables frame switching from one client to another on a WLAN
### 4.1.90.2.13 client-load-balancing

#### wlan-mode commands

Enforces client load balancing on a WLAN’s access point radios. AP6522, AP6532, AP6562, AP81XX, and AP82XX models can support 256 clients per access point. AP6511 and AP6521 models can support up to 128 clients per access point. Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another access point radio.

This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
client-load-balancing {allow-single-band-clients|band-discovery-intvl|
capability-ageout-time|max-probe-req|probe-req-intvl}

client-load-balancing {allow-single-band-clients 2.4ghz|5ghz|
band-discovery-intvl <0-10000>|capability-ageout-time <0-10000>}

client-load-balancing {max-probe-req|probe-req-intvl} 2.4ghz|5ghz <0-10000>
```

#### Parameters

- `client-load-balancing` Configures WLAN client load balancing

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-single-band-clients</td>
<td>Optional. Allows single band clients to associate even during load balancing</td>
</tr>
<tr>
<td>[2.4ghz</td>
<td>5ghz]</td>
</tr>
<tr>
<td></td>
<td>• 5ghz – Enables load balancing across 5.0 GHz channels</td>
</tr>
<tr>
<td></td>
<td>This option is enabled by default for 2.4 and 5.0 GHz radios.</td>
</tr>
<tr>
<td>band-discovery-intvl</td>
<td>Optional. Configures the interval to discover a client's band capability before connection</td>
</tr>
<tr>
<td>&lt;0-10000&gt;</td>
<td>• &lt;0-10000&gt; – Specify a value from 0 - 10000 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td>capability-ageout-time</td>
<td>Optional. Configures a client's capability ageout interval</td>
</tr>
<tr>
<td>&lt;0-10000&gt;</td>
<td>• &lt;0-10000&gt; – Specify a value from 0 - 10000 seconds. The default is 3600 seconds.</td>
</tr>
</tbody>
</table>

- `client-load-balancing {max-probe-req|probe-req-intvl} [2.4ghz|5ghz] <0-10000>`
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>probe-req-intvl</code></td>
<td>Optional. Configures client probe request interval limits for device association</td>
</tr>
<tr>
<td>`[2.4ghz</td>
<td>5ghz]`</td>
</tr>
<tr>
<td><code>&lt;0-10000&gt;</code></td>
<td>• 5ghz – Configures the client probe request interval on 5.0 GHz radios</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;0-10000&gt;</code> – Specify a value from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 10 seconds.</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Disables client load balancing on a WLAN’s access point radios</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-wlan-test)#client-load-balancing band-discovery-intvl 2
rfs7000-37FABE(config-wlan-test)#client-load-balancing probe-req-intvl 5ghz 5
rfs7000-37FABE(config-wlan-test)#show context
wlan test
ssid test
bridging-mode local
encryption-type none
authentication-type eap
accounting syslog host 172.16.10.4 port 2
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back
acl exceed-rate wireless-client-denied-traffic 20 disassociate
broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```
4.1.90.2.14 controller-assisted-mobility

Enables controller or service platform assisted mobility to determine a wireless client’s VLAN assignment. When enabled, a controller or service platform’s mobility database is used to assist in roaming between RF Domains. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
controller-assisted-mobility

Parameters
None

Examples
rfs4000-229D58(config-wlan-test)#controller-assisted-mobility

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables controller or service platform assisted mobility to determine a wireless client’s VLAN assignment</td>
</tr>
</tbody>
</table>
4.1.90.2.15 data-rates

Specifies the 802.11 rates supported on a WLAN

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

data-rates [2.4GHz|5GHz]
data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
data-rates 2.4GHz custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]
data-rates 5GHz [a-only|an|custom|default]
data-rates 5GHz custom [12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]

Parameters
- data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
- data-rates 5GHz [a-only|an|default]

<table>
<thead>
<tr>
<th>data-rates 2.4GHz</th>
<th>Specifies the 802.11 rates supported when mapped to a 2.4 GHz radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>b-only</td>
<td>Uses rates that support only 11b clients</td>
</tr>
<tr>
<td>bg</td>
<td>Uses rates that support both 11b and 11g clients</td>
</tr>
<tr>
<td>bgn</td>
<td>Uses rates that support 11b, 11g and 11n clients</td>
</tr>
<tr>
<td>default</td>
<td>Uses the default rates configured for a 2.4 GHz radio</td>
</tr>
<tr>
<td>g-only</td>
<td>Uses rates that support operation in 11g only</td>
</tr>
<tr>
<td>gn</td>
<td>Uses rates that support 11g and 11n clients</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>data-rates 5GHz</th>
<th>Specifies the 802.11 rates supported when mapped to a 5.0 GHz radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-only</td>
<td>Uses rates that support operation in 11a only</td>
</tr>
<tr>
<td>an</td>
<td>Uses rates that support 11a and 11n clients</td>
</tr>
<tr>
<td>default</td>
<td>Uses default rates configured for a 5.0 GHz</td>
</tr>
</tbody>
</table>

- data-rates [2.4GHz|5GHz] custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]
### custom

Configures a data rates list by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11').

The data-rates for 2.4 GHz and 5.0 GHz channels are the same with a few exceptions. The 2.4 GHz channel has a few extra data rates: 1, 11, 2, and 5.5.

### 1,11,2,5.5

The following data rates are specific to the 2.4 GHz channel:
- 1 – 1-Mbps
- 11 – 11-Mbps
- 2 – 2-Mbps
- 5.5 – 5.5-Mbps

### [12,18,24,36,48,54,6,9,basic-1,basic-11, basic-12,basic-18, basic-2,basic-36, basic-48,basic-5.5, basic-54,basic-6, basic-9, basic-mcs-1s, mcs-1s,mcs2s, mcs-3s]

The following data rates are common to both the 2.4 GHz and 5.0 GHz channels:
- 12 – 12 Mbps
- 18 – 18-Mbps
- 24 – 24 Mbps
- 36 – 36-Mbps
- 48 – 48-Mbps
- 54 – 54-Mbps
- 6 – 6-Mbps
- 9 – 9-Mbps
- basic-1 – basic 1-Mbps
- basic-11 – basic 11-Mbps
- basic-12 – basic 12-Mbps
- basic-18 – basic 18-Mbps
- basic-2 – basic 2-Mbps
- basic-36 – basic 36-Mbps
- basic-48 – basic 48-Mbps
- basic-5.5 – basic 5.5-Mbps
- basic-54 – basic 54-Mbps
- basic-6 – basic 6-Mbps
- basic-9 – basic 9-Mbps
- basic-mcs-1s – Modulation and coding scheme data rates for 1 Spatial Stream
- mcs-1s – Applicable to 1-spatial stream data rates
- mcs-2s – Applicable to 2-spatial stream data rates
- mcs-3s – Applicable to 3-spatial stream data rates
**Examples**

rfs7000-37FABE(config-wlan-test)#data-rates 2.4GHz gn

rfs7000-37FABE(config-wlan-test)#show context
wlan test
ssid test
bridging-mode local
encryption-type none
authentication-type eap
accounting syslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back
acl exceed-rate wireless-client-denied-traffic 20 disassociate
broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the 802.11 data rates supported on a WLAN for the 2.4 GHz or 5.0 GHz radios</td>
</tr>
</tbody>
</table>
### 4.1.90.2.16 description

**wlan-mode commands**

Defines the WLAN description

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

description <LINE>

**Parameters**

- description <LINE>

<table>
<thead>
<tr>
<th>&lt;LINE&gt;</th>
<th>Specify a WLAN description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The WLAN's description should help differentiate it from others with similar configurations. The description should not exceed 64 characters.</td>
</tr>
</tbody>
</table>

**Examples**

```
    rfs7000-37FABE(config-wlan-test)#description TestWLAN
    rfs7000-37FABE(config-wlan-test)#show context wlan test
    description TestWLAN
    ssid test
    bridging-mode local
    encryption-type none
    authentication-type eap
    accounting syslog host 172.16.10.4 port 2
    data-rates 2.4GHz gn
    client-load-balancing probe-req-intvl 5ghz 5
    client-load-balancing band-discovery-intvl 2
    captive-portal-enforcement fall-back
    acl exceed-rate wireless-client-denied-traffic 20 disassociate
    broadcast-dhcp validate-offer
    rfs7000-37FABE(config-wlan-test)#
```

**Related Commands**

| no | Removes a WLAN's configured description |
4.1.90.2.17 downstream-group-addressed-forwarding

wlan-mode commands

Enables forwarding of downstream broadcast/multicast (BC/MC) packets to a group on this WLAN. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
downstream-group-addressed-forwarding

Parameters
None

Examples
rfs4000-229D58(config-wlan-test)#downstream-group-addressed-forwarding
rfs4000-229D58(config-wlan-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables forwarding of downstream BCMC packets to a group on this WLAN</td>
</tr>
</tbody>
</table>
4.1.90.2.18 dynamic-vlan-assignment

* wlan-mode commands *

Enables dynamic VLAN assignment on this WLAN. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dynamic-vlan-assignment allowed-vlans <VLAN-ID>

**Parameters**
- dynamic-vlan-assignment allowed-vlans <VLAN-ID>

<table>
<thead>
<tr>
<th>dynamic-vlan-assignment allowed-vlans</th>
<th>Enables dynamic VLAN assignment and configures a list of VLAN IDs or VLAN alias allowed access to the WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VLAN-ID&gt;</td>
<td>Specify the list of VLAN IDs or the VLAN alias names. For example, 10-20, 25, 30-35, $guest. For information on VLAN aliases, see alias.</td>
</tr>
</tbody>
</table>

**Examples**

rfs4000-229D58(config-wlan-test)#dynamic-vlan-assignment allowed-vlans 10-20

rfs4000-229D58(config-wlan-test)#show context
wlan test
ssid test
bridging-mode tunnel
encryption-type none
authentication-type none
dynamic-vlan-assignment allowed-vlans 10-20
rfs4000-229D58(config-wlan-test)#

**Related Commands**

| no     | Disables dynamic VLAN assignment on this WLAN |
4.1.90.2.19 eap-types

- **wlan-mode commands**

Configures client access based on the EAP type used

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls]
{(aka|all|fast|peap|sim|tls|ttls)}
```

**Parameters**

- `eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls]`

| eap-types [allow|deny] | Configures a list of allowed or denied EAP types |
|------------------------|-----------------------------------------------|
| • allow                | Configures a list of EAP types allowed for WLAN client authentication |
| • deny                 | Configures a list of EAP types not allowed for WLAN client authentication |

| [aka|all|fast|peap|sim|tls|ttls] | The following EAP types are common to the ‘allow’ and ‘deny’ keywords: |
|----------------------------------------|---------------------------------------------------------------------|
| • aka – Configures EAP Authentication and Key Agreement (AKA) and EAP-AKA’ (AKA Prime). EAP-AKA is one of the methods in the EAP authentication framework. It uses Universal Mobile Telecommunications System (UMTS) and Universal Subscriber Identity Module (USIM) for client authentication and key distribution. |
| • all – Allows or denies usage of all EAP types on the WLAN. This is the default setting. |
| • peap – Configures Protected Extensible Authentication Protocol (PEAP). PEAP or Protected EAP uses encrypted and authenticated TLS tunnel to encapsulate EAP. |
| • sim – Configures EAP Subscriber Identity Module (SIM). EAP-SIM uses Global System for Mobile Communications (GSMC) SIM for client authentication and key distribution. |
| • tls – Configures EAP Transport Layer Security (TLS). EAP-TLS is an EAP authentication method that uses PKI to communicate with a RADIUS server or any other authentication server. |
| • ttls – Configures Tunneled Transport Layer Security (TTLS). EAP-TTLS is an extension of TLS. Unlike TLS, TTLS does not require every client to generate and install a CA- signed certificate. |

**Note:** These options are recursive, and more than one EAP type can be selected. The selected options are added to the allowed or denied EAP types list.
Examples

rfs7000-37FABE(config-wlan-test)#eap-types allow fast sim tls

rfs7000-37FABE(config-wlan-test)#show context
  wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  eap-types allow fast sim tls
rfs7000-37FABE(config-wlan-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reverts to default setting - eap-types allow all</td>
</tr>
</tbody>
</table>
4.1.90.2.20 encryption-type

Sets a WLAN's encryption type

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
encryption-type [ccmp|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]
```

Parameters

- encryption-type [ccmp|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]

<table>
<thead>
<tr>
<th>encryption-type</th>
<th>Configures the WLAN's data encryption parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmp</td>
<td>Configures Advanced Encryption Standard (AES) Counter Mode CBC-MAC Protocol (AES-CCM/CCMP)</td>
</tr>
<tr>
<td>keyguard</td>
<td>Configures Keyguard-MCM (Mobile Computing Mode)</td>
</tr>
<tr>
<td>none</td>
<td>No encryption used. This is the default setting.</td>
</tr>
<tr>
<td>tkip-ccmp</td>
<td>Configures the TKIP and AES-CCM/CCMP encryption modes</td>
</tr>
<tr>
<td>wep128</td>
<td>Configures WEP with 128 bit keys</td>
</tr>
<tr>
<td>wep128-keyguard</td>
<td>Configures WEP128 as well as Keyguard-MCM encryption modes</td>
</tr>
<tr>
<td>wep64</td>
<td>Configures WEP with 64 bit keys. A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption while the other uses WEP.</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-wlan-test)#encryption-type tkip-ccmp
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  description TestWLAN
  ssid test
  bridging-mode local
  encryption-type tkip-ccmp
  authentication-type eap
  accounting syslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
  client-load-balancing probe-req-intvl 5ghz 5
  client-load-balancing band-discovery-intvl 2
  captive-portal-enforcement fall-back
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
  broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```

Related Commands

- no Reset the WLAN's encryption type to default (none)
4.1.90.2.21 enforce-dhcp

▶ wlan-mode commands

Enables dropping of packets from clients with a static IP address. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

enforce-dhcp

Parameters

None

Examples

rfs7000-37FABE(config-wlan-test)#enforce-dhcp

rfs7000-37FABE(config-wlan-test)#show context wlan test
description TestWLAN
ssid test
bridging-mode local
encryption-typetkip-ccmp
authentication-type eap
accountingsyslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back
acl exceed-rate wireless-client-denied-traffic 20 disassociate

enforce-dhcp

broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#

Related Commands

| no | Disables dropping of packets from clients with a static IP address |
4.1.90.2.22 **fast-bss-transition**

* wlan-mode commands

Enables support for 802.11r *Fast-BSS Transition* (FT) on the selected WLAN. This feature is disabled by default. 802.11r is an attempt to undo the burden that security and QoS added to the handoff process, and restore it back to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks. 802.11r FT redefines the security key negotiation protocol, allowing parallel processing of negotiation and requests for wireless resources.

Enabling FT standards provides wireless clients fast, secure and seamless transfer from one base station to another, ensuring continuous connectivity.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`fast-bss-transition {over-ds}`

**Parameters**

- `fast-bss-transition {over-ds}`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>over-ds</td>
<td>Enables 802.11r FT support on this WLAN</td>
</tr>
<tr>
<td>over-ds</td>
<td>• over-ds – Optional. Enables 802.11r client roaming over the <em>Distribution System</em> (DS). When enabled, all client communication with the target AP is via the current AP. This communication, carried in FT action frames, is first sent by the client to the current AP, then forwarded to the target AP through the controller.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-wlan-test)#fast-bss-transition
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  vlan 1
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  fast-bss-transition
rfs7000-37FABE(config-wlan-test)#
```

**Related Commands**

- **no** Disables support for 802.11r *Fast-BSS Transition* (FT) on a WLAN
4.1.90.2.23 http-analyze

* wlan-mode commands *

Enables HTTP URL analysis on the WLAN

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

http-analyze [filter|syslog]
http-analyze filter [images|post|query-string]
http-analyze syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}

**Parameters**

- **http-analyze filter [images|post|query-string]**
  - filter: Filters URLs, based on the parameters set, before forwarding them
  - images: Filters out URLs referring to images (does not forward URL requesting images)
  - post: Filters out URLs requesting POST (does not forward POST requests). This option is disabled by default.
  - query-string: Removes query strings from URLs before forwarding them (forwards requests and no data). This option is disabled by default.

- **http-analyze syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}

**Examples**

rfs4000-229D58(config-wlan-test)#http-analyze syslog host 192.168.13.10 port 21 proxy-mode through-controller

rfs4000-229D58(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  http-analyze syslog host 192.168.13.10 port 21 proxy-mode through-controller
rfs4000-229D58(config-wlan-test)
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables HTTP URL analysis on the WLAN</td>
</tr>
</tbody>
</table>
4.1.90.2.24 ip

wlan-mode commands

Configures Internet Protocol (IP) settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ip [arp|dhcp]

ip arp [header-mismatch-validation|trust]

ip dhcp trust

Parameters

- ip arp [header-mismatch-validation|trust]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp</td>
<td>Configures the IP settings for ARP packets</td>
</tr>
<tr>
<td>header-mismatch-</td>
<td>Verifies mismatch of source MAC address in the</td>
</tr>
<tr>
<td>validation</td>
<td>ARP and Ethernet headers. This option is</td>
</tr>
<tr>
<td>trust</td>
<td>enabled by default.</td>
</tr>
<tr>
<td>trust</td>
<td>Sets ARP responses as trusted for a WLAN/range.</td>
</tr>
<tr>
<td></td>
<td>This option is disabled by default.</td>
</tr>
</tbody>
</table>

- ip dhcp trust

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp</td>
<td>Configures the IP settings for DHCP packets</td>
</tr>
<tr>
<td>trust</td>
<td>Sets DHCP responses as trusted for a WLAN/range.</td>
</tr>
<tr>
<td></td>
<td>This option is disabled by default.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-wlan-test)#ip dhcp trust

rfs7000-37FABE(config-wlan-test)#show context
wlan test
description TestWLAN
ssid test
bridging-mode local
encryption-type tkip-ccmp
authentication-type eap
accounting syslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back
ip dhcp trust
acl exceed-rate wireless-client-denied-traffic 20 disassociate
enforce-dhcp
broadcast-dhcp validate-offer
http-analyze controller
rfs7000-37FABE(config-wlan-test)#

Related Commands

no Reset IP ARP or DHCP trust parameters to default. ARP trust is disabled, ARP mismatch verification is enabled, or DHCP trust is disabled.
4.1.90.2.25 ipv6

Sets the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this WLAN

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

Syntax

ipv6 [dhcpv6|nd]
ipv6 dhcpv6 trust
ipv6 nd [header-mismatch-validation|raguard|trust]

Parameters

- ipv6 dhcpv6 trust
- ipv6 nd [header-mismatch-validation|raguard|trust]

<table>
<thead>
<tr>
<th>ipv6 dhcpv6 trust</th>
<th>Enables DHCPv6 trust state for DHCPv6 responses on this WLAN. When enabled, all DHCPv6 responses received on this WLAN are trusted and forwarded. This option is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd [header-mismatch-validation</td>
<td>raguard</td>
</tr>
<tr>
<td>ipv6 nd</td>
<td>Sets the IPv6 ND settings for this WLAN</td>
</tr>
<tr>
<td>header-mismatch-validation</td>
<td>Checks for mismatch of source MAC address in the ICMPv6 ND message and Ethernet header (link layer option). This option is enabled by default.</td>
</tr>
<tr>
<td>raguard</td>
<td>Allows redirection of router advertisements (RAs) and ICMPv6 packets originating on this WLAN. This option is disabled by default.</td>
</tr>
<tr>
<td>trust</td>
<td>Enables trust state for ND requests received on this WLAN. When enabled, all ND requests on an IPv6 firewall, on this WLAN, are trusted. This option is disabled by default.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-wlan-test)#ipv6 dhcpv6 trust
rfs7000-37FABE(config-wlan-test)#ipv6 nd trust
rfs7000-37FABE(config-wlan-test)#show context wlan test
  ssid test
  vlan 1
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  ipv6 dhcpv6 trust
  ipv6 nd trust
rfs7000-37FABE(config-wlan-test)#

Related Commands

no | Resets IPv6 ND or DHCPv6 trust parameters to default. ND request trust is disabled, ND header mismatch verification is enabled, ND RA and ICMPv6 redirection is disabled, or DHCPv6 trust is disabled. |
4.1.90.2.26  kerberos

wlan-mode commands

Configures Kerberos authentication parameters on a WLAN

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.

Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with 802.11b clients. Kerberos uses Network Time Protocol (NTP) for synchronizing the clocks of its Key Distribution Center (KDC) server(s).

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

kerberos [password|realm|server]
kerberos password [0 <LINE>|2 <LINE>|<LINE>]
kerberos realm <REALM>
kerberos server [primary|secondary|timeout]
kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}
kerberos server timeout <1-60>

Parameters
- kerberos password [0 <LINE>|2 <LINE>|<LINE>]
- kerberos realm <REALM>
- kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}

<table>
<thead>
<tr>
<th>kerberos</th>
<th>Configures a WLAN’s Kerberos authentication parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The parameters are: password, realm, and server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>password</th>
<th>Configures a Kerberos KDC server password. The password should not exceed 127 characters. The password options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 0 &lt;LINE&gt; – Configures a clear text password</td>
</tr>
<tr>
<td></td>
<td>• 2 &lt;LINE&gt; – Configures an encrypted password</td>
</tr>
<tr>
<td></td>
<td>• &lt;LINE&gt; – Specify the password.</td>
</tr>
</tbody>
</table>

| kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>} | Configures a WLAN’s Kerberos authentication parameters |
|-------------------------------------------------------------|-----------------------------------------------------|
|                                                             | The parameters are: password, realm, and server.     |
**server**

<table>
<thead>
<tr>
<th>Config</th>
<th>Description</th>
</tr>
</thead>
</table>
| [primary|secondary] | Configures the primary and secondary KDC server parameters  
  - primary – Configures the primary KDC server parameters  
  - secondary – Configures the secondary KDC server parameters |

**host <IP/HOSTNAME>**

<table>
<thead>
<tr>
<th>Config</th>
<th>Description</th>
</tr>
</thead>
</table>
| Sets the primary or secondary KDC server address  
  - <IP/HOSTNAME> – Specify the IP address or name of the KDC server. |

**port <1-65535>**

<table>
<thead>
<tr>
<th>Config</th>
<th>Description</th>
</tr>
</thead>
</table>
| Optional. Configures the UDP port used to connect to the KDC server  
  - <1-65535> – Specify the port from 1 - 65535. The default is 88. |

**Examples**

```
rfs7000-37FABE(config-wlan-test)#kerberos server timeout 12
rfs7000-37FABE(config-wlan-test)#kerberos server primary host 172.16.10.2 port 88
rfs7000-37FABE(config-wlan-test)#show context
wlan test
description TestWLAN
ssid test
bridging-mode local
encryption-type tkip-ccmp
authentication-type eap
kerberos server timeout 12
kerberos server primary host 172.16.10.2
accounting syslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back
ip dhcp trust
acl exceed-rate wireless-client-denied-traffic 20 disassociate
enforce-dhcp
broadcast-dhcp validate-offer
http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Config</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes Kerberos authentication related parameters on a WLAN</td>
</tr>
</tbody>
</table>
4.1.90.2.27  mac-authentication

Enables MAC authentication. When enabled, the system uses cached credentials (RADIUS server lookups are skipped) to authenticate clients.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
mac-authentication [cached-credentials|enforce-always]

Parameters
- mac-authentication [cached-credentials|enforce-always]
  - cached-credentials: Uses cached credentials to skip RADIUS lookups. This option is disabled by default.
  - enforce-always: Enforces MAC authentication on this WLAN. When enabled, MAC authentication is enforced, each time a client logs in, even when the authentication type specified (using the authentication-type command) is not MAC authentication. This option is disabled by default.

Examples
rfs4000-229D58(config-wlan-test)#mac-authentication cached-credentials
rfs4000-229D58(config-wlan-test)#

Related Commands
no
  Disables MAC authentication related parameters: Disables use of cached credentials to skip RADIUS lookups, or disables enforcement of MAC authentication on this WLAN.
4.1.90.2.28  no

Negates WLAN mode commands and reverts values to their default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax


no accounting [radius|syslog|wait-client-ip]
no acl exceed-rate wireless-client-denied-traffic

no assoc-response [deny-threshold|rssi-threshold]
no http-analyze {filter|syslog}
no http-analyze {filter [images|post|query-string]}
no ip [arp|dhcp]
no ip arp [header-mismatch-validation|trust]
no ip dhcp trust

no ipv6 [dhcpp6|nd]
no ipv6 dhcpp6 trust
no ipv6 nd [header-mismatch-validation|guard|trust]

no kerberos [password|realm|server]
no kerberos server [primary host|secondary host|timeout]
no mac-authentication [cached-credentials|enforce-always]
no radio-resource-measurement {channel-report|neighbor-report {hybrid}}
no radius [dynamic-authorization|nas-identifier|nas-port-id|vlan-assignment]
no registration {external}
no relay-agent [dhcp-option82|dhcppv6-ldra]

no shutdown {on-critical-resource|on-meshpoint-loss|on-primary-port-link-loss|on-unadoption}
no time-based-access days [all|friday|monday|saturday|sunday|thursday|tuesday|
  wednesday|weekdays|weekends]

no use [aaa-policy|association-acl-policy|bonjour-gw-discovery-policy|captive-portal|
  ip-access-list|ipv6-access-list|mac-access-list|passpoint-policy|
  roaming-assist-policy|url-filter|wlan-qos-policy]

no vlan-pool-member [<1-40 95>|<VLAN-ALIAS-NAME>]

no [wep128|wep64] [key {1-4}|transmit-key]

no wing-extension [move-command|smart-scan|wing-load-information|
  wmm-load-information]

no wireless-client [count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|
  max-firewall-sessions|reauthentication|roam-notification|t5-inactivity-timeout|
  tx-power|vlan-cache-ageout]

Parameters
- no <PARAMETERS>

no <PARAMETERS> Removes or reverts this WLAN's settings based on the parameters passed

Usage Guidelines
The no command negates any command associated with it. Wherever required, use the same parameters
associated with the command getting negated.

Examples
rfs7000-37FABE (config-wlan-test)#no?
  accounting Configure how accounting records are
  created for this wlan
  acl Actions taken based on ACL
  configuration [ packet drop being one
  of them]
  answer-broadcast-probes Do not Include this wlan when
  responding to probe requests that do
  not specify an SSID
  assoc-response Association response threshold
  association-list Configure the association list for
  the wlan
  authentication-type Reset the authentication to use on
  this wlan to default (none/Pre-shared
  keys)
  broadcast-dhcp Configure broadcast DHCP packet
  handling
  broadcast-ssid Do not advertise the SSID of the WLAN
  in beacons
  captive-portal-enforcement Configure how captive-portal is
  enforced on the wlan
  client-access Disallow client access on this wlan
  (no data operations)
  client-client-communication Disallow switching of frames from one
  wireless client to another on this
  wlan
  client-load-balancing Disable load-balancing of clients on
  this wlan
  controller-assisted-mobility Disable configure assisted mobility
  data-rates Reset data rate configuration to
default
  description Reset the description of the wlan
  downstream-group-addressed-forwarding Disable downstream group addressed
  forwarding of packets
  dynamic-vlan-assignment Dynamic VLAN assignment configuration
  eap-types Allow all EAP types on this wlan
  encryption-type Reset the encryption to use on this
  wlan to default (none)
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enforce-dhcp</td>
<td>Drop packets from Wireless Clients with static IP address</td>
</tr>
<tr>
<td>fast-bss-transition</td>
<td>Disable support for 802.11r Fast BSS Transition</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enable HTTP URL analysis on the wlan</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>ipv6</td>
<td>Internet Protocol version 6 (IPv6)</td>
</tr>
<tr>
<td>kerberos</td>
<td>Configure kerberos authentication parameters</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>Configure mac-authentication related parameters</td>
</tr>
<tr>
<td>opendns</td>
<td>OpenDNS related config for this wlan</td>
</tr>
<tr>
<td>proxy-arp-mode</td>
<td>Configure handling of ARP requests with proxy-arp is enabled</td>
</tr>
<tr>
<td>proxy-nd-mode</td>
<td>Configure handling of IPv6 ND requests with proxy-nd is enabled</td>
</tr>
<tr>
<td>qos-map</td>
<td>Disable the 802.11u QoS map element and frame</td>
</tr>
<tr>
<td>radio-resource-measurement</td>
<td>Disable support for 802.11k Radio Resource Measurement</td>
</tr>
<tr>
<td>radius registration</td>
<td>Configure RADIUS related parameters</td>
</tr>
<tr>
<td>registration</td>
<td>Dynamic registration of device (or) user</td>
</tr>
<tr>
<td>relay-agent</td>
<td>Configure dhcp relay agent info</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enable the use of this wlan</td>
</tr>
<tr>
<td>ssid</td>
<td>Configure ssid</td>
</tr>
<tr>
<td>t5-client-isolation</td>
<td>Do not Isolate traffic among clients</td>
</tr>
<tr>
<td>t5-security</td>
<td>Configure encryption and authentication</td>
</tr>
<tr>
<td>time-based-access</td>
<td>Reset time-based-access parameters to default</td>
</tr>
<tr>
<td>use</td>
<td>Set setting to use</td>
</tr>
<tr>
<td>vlan</td>
<td>Map the default vlan (vlan-id 1) to the wlan</td>
</tr>
<tr>
<td>vlan-pool-member</td>
<td>Delete a mapped vlan from this wlan</td>
</tr>
<tr>
<td>wep128</td>
<td>Reset WEP128 parameters</td>
</tr>
<tr>
<td>wep64</td>
<td>Reset WEP64 parameters</td>
</tr>
<tr>
<td>wing-extensions</td>
<td>Disable support for WiNG-Specific enhancements to 802.11</td>
</tr>
<tr>
<td>wireless-client</td>
<td>Configure wireless-client specific parameters</td>
</tr>
<tr>
<td>wpa-wpa2</td>
<td>Modify tkip-ccmp (wpa/wpa2) related parameters</td>
</tr>
<tr>
<td>service</td>
<td>Service to monitor to show no-service page to user</td>
</tr>
</tbody>
</table>

The test settings before execution of the no command:

```
rfs7000-37FABE(config-wlan-test)#
rfs7000-37FABE(config-wlan-test)#show context
wlan test
description TestWLAN
ssid test
bridging-mode local
encryption-type tkip-ccmp
authentication-type eap
kerberos server timeout 12
kerberos server primary host 172.16.10.2
accounting syslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back
ip dhcp trust
acl exceed-rate wireless-client-denied-traffic 20 disassociate
```
enforce-dhcp
  broadcast-dhcp validate-offer
  http-analyze controller
rfs7000-37FABE(config-wlan-test)#

rfs7000-37FABE(config-wlan-test)#no accounting syslog
rfs7000-37FABE(config-wlan-test)#no description
rfs7000-37FABE(config-wlan-test)#no authentication-type
rfs7000-37FABE(config-wlan-test)#no encryption-type
rfs7000-37FABE(config-wlan-test)#no enforce-dhcp
rfs7000-37FABE(config-wlan-test)#no kerberos server primary host
rfs7000-37FABE(config-wlan-test)#no kerberos server timeout
rfs7000-37FABE(config-wlan-test)#no data-rates 2.4GHz
rfs7000-37FABE(config-wlan-test)#no ip dhcp trust
rfs7000-37FABE(config-wlan-test)#no captive-portal-enforcement

The test settings after the execution of the no command:
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode local
  encryption-type none
  authentication-type none
  wing-extensions wmm-load-information
  client-load-balancing probe-req-intvl 5ghz 5
  client-load-balancing band-discovery-intvl 2
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
  broadcast-dhcp validate-offer
  http-analyze controller
rfs7000-37FABE(config-wlan-test)#

Related Commands

no
4.1.90.2.29 opendns

Enables integration of access points, wireless controllers, and service platforms with OpenDNS. When configured, DNS queries from wireless clients are redirected to OpenDNS (208.67.220.220 OR 208.67.222.222). These OpenDNS resolvers act as proxy DNS servers that provide additional functionalities, such as Web filtering, reporting, and performance enhancement.

This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

opendns device-id <DEVICE-ID>

Parameters

- opendns device-id <DEVICE-ID>

<table>
<thead>
<tr>
<th>opendns device-id &lt;DEVICE-ID&gt;</th>
<th>Configures the device ID sent to OpenDNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DEVICE-ID&gt; – Specify the device ID. The device-id entered here is obtained from the OpenDNS site by executing the following command in the Privi Exec Mode: <code>opendns &gt; username &lt;WORD&gt; password &lt;WORD. label &lt;WORD&gt;</code>. For more information, see <code>opendns</code>.</td>
<td></td>
</tr>
<tr>
<td>Once configured on a WLAN, this value is embedded in each DNS query packet going out from an access point, wireless controller, or service platform to the OpenDNS server. The device ID is a sixteen (16) character hex string representing a 64 bit unsigned integer. Use the <code>no &gt; opendns &gt; device-id</code> command to remove the configured device-id.</td>
<td></td>
</tr>
<tr>
<td>Therefore, when a wireless client associates with a OpenDNS enabled WLAN, all DNS queries originating from the client are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> To enable redirection of DNS query to OpenDNS it is necessary that the DNS server's IP address provided in the DHCP Server policy (used by the client) should point to the OpenDNS IP address (208.67.220.220 OR 208.67.222.222). For more information, see <code>dns-server</code>.</td>
<td></td>
</tr>
<tr>
<td>For example: <code>dns-server</code></td>
<td></td>
</tr>
<tr>
<td>Contd...</td>
<td></td>
</tr>
</tbody>
</table>
Examples
Following examples show all configurations required to integrate access points and controllers with the OpenDNS service:

Step 1. In the Privilege Executable Mode:

```bash
ap7131-E6D512#opendns username bob@examplecompany.com password opendns label company_name
Connecting to OpenDNS server...
device_id = 0014AADF8EDC6C59
ap7131-E6D512#
```

Step 2: To enable OpenDNS on a WLAN, apply the device-id, obtained in the preceding step, to the WLAN:

```bash
ap7131-E6D512(config)#wlan opendns
ap7131-E6D512(config-wlan-opendns)#opendns device-id 0014AADF8EDC6C59
ap7131-E6D512(config-wlan-opendns)#commit
ap7131-E6D512(config-wlan-opendns)#show context
```

The following examples show the other mandatory configurations needed to redirect wireless client DNS queries to the OpenDNS server:

```bash
ap7131-E6D512(config)#self
ap7131-E6D512(config-device-00-15-70-E6-D5-12)#
```

Step 3: To enable DNS resolution on the access point or controller, execute the following commands:

```bash
ap7131-E6D512(config-device-00-15-70-E6-D5-12)#ip name-server 144.189.100.51
ap7131-E6D512(config-device-00-15-70-E6-D5-12)#ip dns-server-forward
ap7131-E6D512(config-device-00-15-70-E6-D5-12)#show context
```

Note: To prevent wireless clients from bypassing the OpenDNS resolver by adding their own DNS servers, configure and apply an IP ACL on the access point, wireless controller, or service platform containing the following firewall rules:

```bash
rfs7000-37FABE(config-ip-acl-dns-list)#show context
ip access-list dns-list
  permit udp any host 208.67.222.222 eq dns rule-precedence 1 rule-description "allow dns queries only to OpenDNS"
  deny udp any any eq dns rule-precedence 10 rule-description "block all other dns queries"
  permit ip any any rule-precedence 100 rule-description "allow all other ip packets"
rfs7000-37FABE(config-ip-acl-dns-list)#
```
Step 4: To ensure that the OpenDNS-enabled WLAN’s client’s DNS queries are redirected to the OpenDNS server, execute the following commands:

```
ap7131-E6D512(config)#dhcp-server-policy dhcppolicy
ap7131-E6D512(config-dhcp-policy-dhcppolicy)#dhcp-pool opendns
ap7131-E6D512(config-dhcp-policy-dhcppolicy)#show context
dhcp-server-policy dhcppolicy
dhcp-pool dhcppool
  network 192.168.1.0/24
  address range 192.168.1.160 192.168.1.200
  default-router 192.168.1.105
dns-server 208.67.222.222
ap7131-E6D512(config-dhcp-policy-dhcppolicy)#
ap7131-E6D512(config)#self
ap7131-E6D512(config-device-00-15-70-E6-D5-12)#use dhcp-server-policy dhcppolicy
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the device ID configured to be forwarded to the DNS query</td>
</tr>
</tbody>
</table>
4.1.90.2.30 **protected-mgmt-frames**

* wlan-mode commands

Configures the WLAN's frame protection mode and security association (SA) query parameters. 802.11w provides protection for both unicast management frames and broadcast/multicast management frames. The 'robust management frames' are action, disassociation, and deauthentication frames. The standard provides one security protocol CCMP for protection of unicast robust management frames. Protected management frames (PMF) protocol only applies to robust management frames after establishment of RSNA PTK. Robust management frame protection is achieved by using CCMP for unicast management frames, broadcast/multicast integrity protocol (BIP) for broadcast/multicast management frames and SA query protocol for protection against (re)association attacks.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```bash
protected-mgmt-frames [mandatory|optional|sa-query [attempts <1-10>| timeout <100-1000>]]
```

**Parameters**
- **mandatory**
  - Enforces **protected management frames** (PMF) on this WLAN (management frames are continually optionally protected)
- **optional**
  - Provides PMF only for those clients that support PMF (management frames are optionally protected)
- **sa-query [attempts <1-10>| timeout <100-1000>]**
  - Configures the following SA parameters:
    - attempts <1-10> – Configures the number of SA query attempts from 1 - 10. The default is 5.
    - timeout <100-1000> – Configures the interval, in milliseconds, used to timeout association requests that exceed the defined interval. Specify a value from 100 - 1000 milliseconds. The default value is 201 milliseconds.

**Examples**

```
rfs7000-37FABE(config-wlan-test)#protected-mgmt-frames mandatory
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  protected-mgmt-frames mandatory
rfs7000-37FABE(config-wlan-test)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables enforcement of protected management frames on this WLAN. And reverts protected management frames sa-query timeout and attempts to 201 milliseconds and 5 respectively.</td>
</tr>
</tbody>
</table>
4.1.90.2.31 proxy-arp-mode

Enables proxy ARP mode for handling ARP requests

Proxy ARP is the technique used to answer ARP requests intended for another system. By faking its identity, the access point accepts responsibility for routing packets to the actual destination.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
proxy-arp-mode [dynamic|strict]

Parameters
- proxy-arp-mode [dynamic|strict]

<table>
<thead>
<tr>
<th>proxy-arp-mode</th>
<th>Enables proxy ARP mode for handling ARP requests. The options available are dynamic and strict.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Forwards ARP requests to the wireless side (for which a response could not be proxied). This is the default setting.</td>
</tr>
<tr>
<td>strict</td>
<td>Does not forward ARP requests to the wireless side</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-wlan-test)#proxy-arp-mode strict
rfs7000-37FABE(config-wlan-test)#show context
wlan test
ssid test
bridging-mode local
encryption-type none
authentication-type none
protected-mgmt-frames mandatory
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
acl exceed-rate wireless-client-denied-traffic 20 disassociate
proxy-arp-mode strict
broadcast-dhcp validate-offer
http-analyze controller
rfs7000-37FABE(config-wlan-test)#

Related Commands
- no Reverts the proxy ARP mode to default (dynamic)
### 4.1.90.2.32 proxy-nd-mode

**wlan-mode commands**

Configures the proxy ND mode for this WLAN member clients as either strict or dynamic.

ND proxy is used in IPv6 to provide reachability by allowing a client to act as proxy. Proxy certificate signing can be done either dynamically (requiring exchanges of identity and authorization information) or statically when the network topology is defined.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
proxy-nd-mode [dynamic|strict]
```

**Parameters**

- `proxy-nd-mode [dynamic|strict]`

| proxy-nd-mode [dynamic|strict] | Configures the proxy ND mode for this WLAN member clients. The options are: dynamic and strict  
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | • dynamic – Forwards ND request to wireless for which a response could not be proxied. This is the default value.  
|                               | • strict – Does not forward ND requests to the wireless side  

**Examples**

```plaintext
rfs7000-37FABE(config-wlan-test)#proxy-nd-mode strict
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  wpa-wpa2 server-only-authentication
  proxy-nd-mode strict
  opendns device-id 44-55-66
  rfs7000-37FABE(config-wlan-test)#
```

**Related Commands**

| no | Reverts the proxy ND mode to default (dynamic) |
### 4.1.90.2.33 qos-map

> **wlan-mode commands**

Enables support for 802.11u QoS map element and frames

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
qos-map
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-wlan-test)#qos-map
rfs7000-37FABE(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 qos-map
 wpa-wpa2 server-only-authentication
 proxy-nd-mode strict
 opendns device-id 44-55-66

rfs7000-37FABE(config-wlan-test)#ac
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables support for 802.11u QoS map element and frames</td>
</tr>
</tbody>
</table>
4.1.90.2.34 radio-resource-measurement

wlan-mode commands

Enables support for 802.11k radio resource measurement capabilities (IEEE 802.11k) on this WLAN.

802.11k improves how traffic is distributed. In a WLAN, devices normally connect to the access point with the strongest signal. Depending on the number and location of clients, this arrangement can lead to excessive demand on one access point and underutilization of others, resulting in degradation of overall network performance. With 802.11k, if the access point with the strongest signal is loaded to its capacity, a client connects to an under-utilized access point. Even if the signal is weaker, the overall throughput is greater since it's an efficient use of the network's resources. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
radio-resource-measurement {channel-report|neighbor-report {hybrid}}

Parameters
- radio-resource-measurement {channel-report|neighbor-report {hybrid}}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio-resource-measurement</td>
<td>Enables support for 802.11k radio resource measurement capabilities</td>
</tr>
<tr>
<td>channel-report</td>
<td>Optional. Includes the channel-report element in beacons and probe responses</td>
</tr>
<tr>
<td>neighbor-report {hybrid}</td>
<td>Optional. Enables responding to neighbor-report requests</td>
</tr>
<tr>
<td>• hybrid</td>
<td>Optional. Uses the hybrid model of smart-rf neighbors and roaming frequency to neighbors</td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58 (config-wlan-test)#radio-resource-measurement

rfs4000-229D58 (config-wlan-test)#show context
wlan test
  ssid test
  vlan 1
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  radio-resource-measurement
  controller-assisted-mobility
rfs4000-229D58 (config-wlan-test)#

Related Commands
- no: Disables support for 802.11k radio resource measurement capabilities (IEEE 802.11k) on this WLAN.
4.1.90.2.35 radius

∇ wlan-mode commands

Configures RADIUS related parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

radius [dynamic-authorization|nas-identifier|nas-port-id|vlan-assignment]

radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id <NAS-PORT-ID>|vlan-assignment]

Parameters

- radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id <NAS-PORT-ID>|vlan-assignment]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-authorization</td>
<td>Enables support for disconnect and change of authorization messages (RFC5176). When enabled, this option extends the RADIUS protocol to support unsolicited messages from the RADIUS server. These messages allow administrators to issue change of authorization (CoA) messages, which affect session authorization, or disconnect messages (DM) that terminate a session immediately. This option is disabled by default.</td>
</tr>
<tr>
<td>nas-identifier &lt;NAS-ID&gt;</td>
<td>Configures the network access server (NAS) identifier attribute, a value that identifies the access point or controller where the RADIUS messages originate. The value specified here is included in the RADIUS NAS-Identifier field for WLAN authentication and accounting packets.</td>
</tr>
<tr>
<td>nas-port-id &lt;NAS-PORT-ID&gt;</td>
<td>Configures the NAS port ID attribute, a value that identifies the port from where the RADIUS messages originate.</td>
</tr>
<tr>
<td>vlan-assignment</td>
<td>Configures the VLAN assignment of a WLAN. RADIUS VLAN assignment is disabled by default. When enabled, this option assigns clients to the RADIUS server specified VLANs, overriding the WLAN configuration. This option is disabled by default. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS access-accept packet, and this feature is enabled, all client traffic is forwarded on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN specified using the vlan/vlan-pool-member options (in the WLAN config mode) is used. Note: If both the RADIUS VLAN assignment and the post authentication VLAN options are enabled, then RADIUS VLAN assignment takes priority over post authentication VLAN configuration.</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-wlan-test)#radius vlan-assignment

rfs7000-37FABE(config-wlan-test)#show context
wlan test
ssid test
bridging-mode local
encryption-type none
authentication-type none
protected-mgmt-frames mandatory
radius vlan-assignment
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
--More--
rfs7000-37FABE(config-wlan-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables support for disconnect and change of authorization messages. Disables the use of VLAN information received in RADIUS server responses, instead uses the VLAN provided in the WLAN configuration. Removes the NAS identifier and NAS port identifiers configured.</td>
</tr>
</tbody>
</table>
4.1.90.2.36 registration

wlan-mode commands

Configures settings enabling dynamic validation of devices by MAC address to continue the authentication process. When enabled, this option registers a device’s MAC address, and allows direct access to a previously registered device.

Supported in the following platforms:

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

registration [device|device-OTP|external|user]

registration [device|device-OTP|user] group-name <RAD-GROUP-NAME>

{agreement-refresh <0-144000>|expiry-time <1-43800>}

registration external host <IP/HOSTNAME> 

{proxy-mode [none|through-controller|through-rf-domain-manager]}

Parameters

- registration external host <IP/HOSTNAME> 

{proxy-mode [none|through-controller|through-rf-domain-manager]}

<table>
<thead>
<tr>
<th>registration</th>
<th>Enables dynamic user registration. This option is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>external</td>
<td>Forwards user information to an external device (i.e. WLAN authentication is handled by an external controller or access point). Use this option to specify the external controller or access point’s details. This option is disabled by default.</td>
</tr>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Specifies the external controller or access point’s IP address or hostname</td>
</tr>
<tr>
<td>proxy-mode</td>
<td>Optional. Specifies the proxy mode. If a proxy is needed for connection, specify the proxy mode as through-controller, through-rf-domain. If no proxy is needed, select none.</td>
</tr>
</tbody>
</table>
| {none|through-controller|through-rf-domain-manager} | - none – Requests are sent directly to the controller from the requesting device  
  - through-controller – Requests are proxied through the controller configuring the device  
  - through-rf-domain-manager – Requests are proxied through the local RF Domain manager |

registration [device|device-OTP|user] group-name <RAD-GROUP-NAME> 

{agreement-refresh <0-144000>|expiry-time <1-43800>}

<table>
<thead>
<tr>
<th>registration</th>
<th>Enables dynamic user registration</th>
</tr>
</thead>
</table>
| [device|device-OTP|user] | Configures self-registration type for this WLAN. Options include device, user and device-OTP  
  - device-OTP – Use this option for MAC registration of users and provision of a one-time-passcode (OTP). If using this option, set the WLAN authentication type as MAC authentication. In this scenario, captive-portal guest users authenticate using their User ID (e-mail address, mobile number, or member id) and the received OTP in order to complete registration.  
  - device – Use this option when captive portal device registration is through social media. When using this option, ensure that the captive portal is configured for guest user social authentication. For more information, see oauth.  
  - user – Use this option for guest users using one of the following options as their user ID during registration: e-mail address, mobile-number, or member-id. |
Examples

nx9500-6C8809(config-wlan-test)#registration user group-name guest agreement-refresh 14400 expiry-time 2000

nx9500-6C8809(config-wlan-test)#show context wlan test
  ssid test
  bridging-mode local
  encryption-type none
  authentication-type none
  registration user group-name guest expiry-time 2000 agreement-refresh 14400

Related Commands

no
Disables dynamic user registration and removes associated configurations. Also disables forwarding of user information to an external device.
4.1.90.2.37 relay-agent

wlan-mode commands

Enables support for DHCP/DHCPv6 relay agent information (option 82 and DHCPv6-LDRA) feature on this WLAN. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
relay-agent [dhcp-option82|dhcpv6-ldra]
```

Parameters

- relay-agent [dhcp-option82|dhcpv6-ldra]

| relay-agent | Enables support for the following DHCP and DHCPv6 options: option 82 and Lightweight DHCPv6 Relay Agent (LDRA) respectively. When enabled, this feature allows the DHCP/DHCPv6 relay agent to insert the relay agent information option (option 82, LDRA) in client requests forwarded to the DHCP/DHCPv6 server. This information provides the following:
| dhcp-option82 | Enables DHCP option 82. DHCP option 82 provides client physical attachment information. This option is disabled by default.
| dhcpv6-ldra | Enables the DHCPv6 relay agent. The DHCPv6 LDRA allows DHCPv6 messages to be transmitted on existing networks that do not currently support IPv6 or DHCPv6. This option is disabled by default.

Examples

```
rfs4000-229D58(config-wlan-test)#relay-agent dhcp-option82

rfs4000-229D58(config-wlan-test)#show context
wlan test
    ssid test
    vlan 1
    bridging-mode tunnel
    encryption-type none
    authentication-type none
    radio-resource-measurement
    relay-agent dhcp-option82
    controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

```
rfs6000-81701D(config-wlan-test)#relay-agent dhcpv6-ldra

rfs6000-81701D(config-wlan-test)#show context
wlan test
    ssid test
    bridging-mode tunnel
    encryption-type none
    authentication-type none
    relay-agent dhcpv6-ldra
rfs6000-81701D(config-wlan-test)#
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables support for DHCP/DHCPv6 relay agent information (option 82 and DHCPv6-LDRA) feature on this WLAN</td>
</tr>
</tbody>
</table>
4.1.90.2.38 shutdown

Auto shuts down a WLAN

The auto shutdown mechanism helps regulate the availability of a WLAN based on an administrator defined access period. Use this feature to shut down a WLAN on specific days and hours and restrict periods when the WLAN traffic is either not desired or cannot be properly administrated. The normal practice is to shut down WLANs when there are no users on the network, such as after hours, weekends or holidays. This allows administrators more time to manage mission critical tasks since the WLAN's availability is automated.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
shutdown {on-critical-resource|on-meshpoint-loss|on-primary-port-link-loss|on-unadoption}
```

Parameters

- shutdown {on-critical-resource|on-meshpoint-loss|on-primary-port-link-loss|on-unadoption}

<table>
<thead>
<tr>
<th>shutdown</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on-critical-resource</td>
<td>Optional. Auto shuts down the WLAN when critical resource failure occurs. Disabled by default.</td>
</tr>
<tr>
<td>on-meshpoint-loss</td>
<td>Optional. Auto shuts down the WLAN when the root meshpoint link fails (is unreachable). Disabled by default.</td>
</tr>
<tr>
<td>on-primary-port-link-loss</td>
<td>Optional. Auto shuts down the WLAN when a device losses its primary Ethernet port (ge1/up1) link. Disabled by default.</td>
</tr>
<tr>
<td>on-unadoption</td>
<td>Optional. Auto shuts down the WLAN when an adopted device becomes unadopted. Disabled by default.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the shutdown on-meshpoint-loss feature is enabled, the WLAN status changes only if the meshpoint and the WLAN are mapped to the same VLAN. If the meshpoint is mapped to VLAN 1 and the WLAN is mapped to VLAN 2, then the WLAN status does not change on loss of the meshpoint.

Examples

```
rfs7000-37FABE(config-wlan-test)#shutdown on-unadoption
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode local
  encryption-type none
  authentication-type none
  protected-mgmt-frames mandatory
  radius vlan-assignment
  wing-extensions wmm-load-information
  client-load-balancing probe-req-intvl 5ghz 5
  client-load-balancing band-discovery-intvl 2
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
  proxy-arp-mode strict
  broadcast-dhcp validate-offer
```
**shutdown on-unadoption**
_http-analyze controller_
_rfs7000-37FABE(config-wlan-test)#_

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables auto shut down WLAN. Use the optional keywords provided to disable auto shut down of the WLAN upon critical resource failure, when meshpoint links fail, when the primary Ethernet port (e1/up1) loses link, or when the WLAN gets unadopted.</td>
</tr>
</tbody>
</table>
4.1.90.2.39  ssid

Wlan-mode commands

Configures a WLAN’s SSID

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ssid <SSID>

Parameters

- ssid <SSID>

<SSID> | Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. Its length should not exceed 32 characters.
---|---

Examples

```
  rfs7000-37FABE(config-wlan-test)#ssid testWLAN1
  rfs7000-37FABE(config-wlan-test)#show context
  wlan test
    ssid testWLAN1
    bridging-mode local
    encryption-type none
    authentication-type none
    protected-mgmt-frames mandatory
    radius vlan-assignment
    wing-extensions wmm-load-information
    client-load-balancing probe-req-intvl 5ghz 5
    client-load-balancing band-discovery-intvl 2
    acl exceed-rate wireless-client-denied-traffic 20 disassociate
    proxy-arp-mode strict
    broadcast-dhcp validate-offer
    shutdown on-unadoption
    http-analyze controller
  rfs7000-37FABE(config-wlan-test)#
```

Related Commands

- **no** | Removes the WLAN’s SSID
### 4.1.90.2.40 t5-client-isolation

**wlan-mode commands**

Disallows clients connecting to the WLAN to communicate with one another. This setting applies exclusively to CPE devices managed by aT5 controller and is disabled by default.

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5’s management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE’s physical wallplate connection and phone jack.

**NOTE:** This setting is applicable only when this WLAN supports T5 controllers and their connected CPEs.

Supported in the following platforms:
- Wireless Controllers — RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

t5-client-isolation

**Parameters**

None

**Examples**

nx9500-6C8809(config-wlan-test)#t5-client-isolation

nx9500-6C8809(config-wlan-test)#show context wlan test ssid test bridging-mode local encryption-type none authentication-type none t5-client-isolation

nx9500-6C8809(config-wlan-test)"

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Allows clients connecting to the WLAN to communicate with one another</td>
</tr>
</tbody>
</table>
4.1.90.2.41 t5-security

* wlan-mode commands

Configures T5 PowerBroadband security settings. A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

**NOTE:** This setting is applicable only when this WLAN supports T5 controllers and their connected CPEs.

Supported in the following platforms:
- Wireless Controllers — RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```shell
    t5-security [static-wep|wpa-enterprise|wpa-personal]
    t5-security static-wep encryption-type [wep128|wep64] [hex <STRING>|passphrase <STRING>]
    t5-security [wpa-enterprise|wpa-personal] encryption-type [ccmp|tkip|tkip-ccmp] version [mixed|wpa|wpa2]
```

**Parameters**

- **t5-security static-wep encryption-type [wep128|wep64] [hex <STRING>|passphrase <STRING>]**
  - `t5-security static-wep` Configures the T5 WLAN security type as static-wep
  - `encryption-type [wep128|wep64]` Applies one of the following encryption algorithms to the T5 support WLAN configuration: WEP64 or WEP128
  - `hex <STRING>` Configures the hex password (used to derive the security key)
    - `<STRING>` – Specify the hex password (should not exceed the 10 - 26 characters).
  - `passphrase <STRING>` Configures the passphrase shared by both transmitting and receiving authenticators
    - `<STRING>` – Specify the passphrase. It could either be an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters. The alphanumeric string allows character spaces. This string is converted to a numeric value. Configuring a passphrase saves you the need to create a 256-bit key each time keys are generated.

- **t5-security [wpa-enterprise|wpa-personal] encryption-type [ccmp|tkip|tkip-ccmp] version [mixed|wpa|wpa2]**
  - `t5-security` Configures the T5 WLAN security type as: wpa-enterprise OR wpa-personal
Examples

```
nx9500-6C8809(config-wlan-test)#t5-security wpa-enterprise encryption-type ccmp
version wpa
```

```
nx9500-6C8809(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode local
  encryption-type none
  authentication-type none
  t5-security wpa-enterprise encryption-type ccmp version wpa
t5-client-isolation
nx9500-6C8809(config-wlan-test)#
```

Related Commands

```
no
```

Removes the configured T5 PowerBroadband security settings
4.1.90.2.42 time-based-access

wlan-mode commands

Configures time-based client access to the network resources

Administrators can use this feature to assign fixed days and time of WLAN access for wireless clients

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9600

Syntax

time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|
saturday|all|weekends|weekdays] {start <START-TIME>} [end <END-TIME>]

Parameters
- day <option> Specifies the day or days on which the client can access the WLAN
  - sunday – Allows access on Sundays only
  - monday – Allows access on Mondays only
  - tuesday – Allows access on Tuesdays only
  - wednesday – Allows access on Wednesdays only
  - thursday – Allows access on Thursdays only
  - friday – Allows access on Fridays only
  - saturday – Allows access on Saturdays only
  - weekends – Allows access on weekends only
  - weekdays – Allows access on weekdays only
  - all – Allows access on all days
- start <START-TIME> Optional. Specifies the access start time in hours and minutes (HH:MM)
- end <END-TIME> Specifies the access end time in hours and minutes (HH:MM)

Usage Guidelines
Ensure the system clock is configured correctly.

Examples
rfs7000-37FABE(config-wlan-test)#time-based-access days weekdays start 10:00 end 16:30
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid testWLAN1
  bridging-mode local
  encryption-type none
  authentication-type none
  protected-mgmt-frames mandatory
  radius vlan-assignment
time-based-access days weekdays start 10:00 end 16:30
  --More--
rfs7000-37FABE(config-wlan-test)#

Related Commands
- no Removes the configured time-based-access settings
4.1.90.2.43 use

Wlan-mode commands

This command associates an existing captive portal with a WLAN.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

use [aaa-policy|application-policy|association-acl-policy|bonjour-gw-discovery-policy|
captive-portal|ip-access-list|ipv6-access-list|mac-access-list|passpoint-policy|
roaming-assist-policy|url-list|wlan-qos-policy]

use [aaa-policy <AAA-POLICY-NAME>|application-policy <POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|
bonjour-gw-discovery-policy <POLICY-NAME>|captive-portal <CAPTIVE-PORTAL-NAME>|
passpoint-policy <PASSPOINT-POLICY-NAME>|
roaming-assist-policy <POLICY-NAME>|
url-filter <URL-FILTER-NAME>|
wlan-qos-policy <WLAN-QoS-POLICY-NAME>]

use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>
use ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>

Parameters

- use [aaa-policy <AAA-POLICY-NAME>|application-policy <POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|
captive-portal <CAPTIVE-PORTAL-NAME>|
passpoint-policy <PASSPOINT-POLICY-NAME>|
roaming-assist-policy <POLICY-NAME>|
url-filter <URL-FILTER-NAME>|
wlan-qos-policy <WLAN-QoS-POLICY-NAME>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-policy &lt;AAA-POLICY-NAME&gt;</td>
<td>Uses an existing AAA policy with a WLAN</td>
</tr>
<tr>
<td></td>
<td>- &lt;AAA-POLICY-NAME&gt; — Specify the AAA policy name.</td>
</tr>
<tr>
<td>application-policy &lt;POLICY-NAME&gt;</td>
<td>Uses an existing application policy with a WLAN.</td>
</tr>
<tr>
<td></td>
<td>- &lt;POLICY-NAME&gt; — Specify the policy name.</td>
</tr>
<tr>
<td>association-acl &lt;ASSOCIATION-NAME&gt;</td>
<td>Uses an existing association ACL policy with a WLAN</td>
</tr>
<tr>
<td></td>
<td>- &lt;ASSOCIATION-NAME&gt; — Specify the association ACL policy name.</td>
</tr>
<tr>
<td>bonjour-gw-discovery-policy &lt;POLICY-NAME&gt;</td>
<td>Uses an existing Bonjour GW Discovery policy with a WLAN. When associated, the Bonjour GW Discovery policy defines a list of services clients can discover across subnets. Bonjour enables discovery of services on a LAN. Bonjour allows the setting up a network (without any configuration) in which services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.</td>
</tr>
<tr>
<td></td>
<td>- &lt;POLICY-NAME&gt; — Specify the Bonjour GW Discovery policy name (should be existing and configured).</td>
</tr>
</tbody>
</table>

Note: For more information on Bonjour GW Discovery policy, see bonjour-gw-discovery-policy.
| captive-portal `<CAPTIVE-PORTAL-NAME>` | Enables a WLAN’s captive portal authentication  
| | • `<CAPTIVE-PORTAL-NAME>` – Specify the captive portal name. |
| **passpoint-policy** `<PASSPOINT-POLICY-NAME>` | Associates a passpoint policy (Hotspot2 configuration) with this WLAN  
| | • `<PASSPOINT-POLICY-NAME>` – Specify the Hotspot 2.0 policy name.  
| | **Note:** For more information on passpoint policy, see `passpoint-policy`.  
| | Map a passpoint policy to a WLAN. Since the configuration gets applied to the radio by BSS, only the Hotspot 2.0 configuration of primary WLANs on a BSSID is used.  
| | Incoming Hotspot 2.0 GAQ/ANQP requests from clients are identified by their destination MAC addresses and are handled by the passpoint policy from the primary WLAN on that BSS.  
| | Define one passpoint policy for every WLAN configured. |
| roamng-assist-policy `<POLICY-NAME>` | Associates an existing roaming assist policy with this WLAN  
| | • `<POLICY-NAME>` – Specify the Roaming Assist policy name.  
| | **Note:** For more information on roaming assist policy, see `roaming-assist-policy`. |
| url-filter `<URL-FILTER-NAME>` | Associates an existing URL list with this WLAN  
| | • `<URL-FILTER-NAME>` – Specify the URL filter name.  
| | **Note:** For more information on configuring a URL list, see `url-list`. |
| wlan-qos-policy `<WLAN-QOS-POLICY-NAME>` | Uses an existing WLAN QoS policy with a WLAN  
| | • `<wlan-qos-policy-name>` – Specify the WLAN QoS policy name. |
| **ip-access-list** [in|out] `<IP-ACCESS-LIST-NAME>` | Specifies the IP access list for incoming and outgoing packets  
| | • in – Applies the IP ACL to incoming packets  
| | • out – Applies IP ACL to outgoing packets  
| | • `<IP-ACCESS-LIST-NAME>` – Specify the IP access list name. |
| **ipv6-access-list** [in|out] `<IPv6-ACCESS-LIST-NAME>` | Specifies the IPv6 access list for incoming and outgoing packets  
| | • in – Applies the IPv6 ACL to incoming packets  
| | • out – Applies IPv6 ACL to outgoing packets  
| | • `<IPv6-ACCESS-LIST-NAME>` – Specify the IPv6 access list name. |
| **mac-access-list** [in|out] `<MAC-ACCESS-LIST-NAME>` | Specifies the MAC access list for incoming and outgoing packets  
| | • in – Applies the MAC ACL to incoming packets  
| | • out – Applies MAC ACL to outgoing packets  
| | • `<MAC-ACCESS-LIST-NAME>` – Specify the MAC access list name. |
Usage Guidelines

IP and MAC ACLs act as firewalls within a WLAN. WLANs use ACLs as firewalls to filter or mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of Access Control Entries (ACEs). Each ACE specifies a set of conditions (rules) and the action taken in case of a match. The action can be permit, deny, or mark. Therefore, when a packet matches an ACE’s conditions, it is either forwarded, dropped, or marked depending on the action specified in the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP ACLs contain deny and permit rules specifying source and destination IP addresses. Each rule has a precedence order assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, you can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny, or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

Examples

```
rfs7000-37FABE(config-wlan-test)#use aaa-policy test

rfs7000-37FABE(config-wlan-test)#use association-acl-policy test

rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid testWLAN1
  bridging-mode local
  encryption-type none
  authentication-type none
  protected-mgmt-frames mandatory
  radius vlan-assignment
  time-based-access days weekdays start 10:00 end 16:30
  wing-extensions wmm-load-information
  client-load-balancing probe-req-intvl 5ghz 5
  client-load-balancing band-discovery-intvl 2
  use aaa-policy test
  use association-acl-policy test
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
  proxy-arp-mode strict
  broadcast-dhcp validate-offer
  shutdown on-unadoption
  http-analyze controller

rfs7000-37FABE(config-wlan-test)#
```

```
rfs7000-37FABE(config-wlan-ipad_clients)#use bonjour-gw-discovery-policy generic

rfs7000-37FABE(config-wlan-ipad_clients)#show context
wlan ipad_clients
  ssid ipad_clients
  vlan 41
  bridging-mode local
  encryption-type none
  authentication-type none
  use bonjour-gw-discovery-policy generic

rfs7000-37FABE(config-wlan-ipad_clients)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the following policies associated with a WLAN: aaa-policy, application-policy, association-acl-policy, bonjour-gw-discovery-policy, captive-portal, ip-access-list, ipv6-access-list, mac-access-list, passpoint-policy, roaming-assist-policy, url-filter, or wlan-qos-policy.</td>
</tr>
</tbody>
</table>
4.1.90.2.44 vlan

Sets the VLAN where traffic from a WLAN is mapped

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

Parameters

- `vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

| <1-4094> | Sets a WLAN's VLAN ID. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased. Use this command to assign just one VLAN to the WLAN. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool. |
| <VLAN-ALIAS-NAME> | Assigns a VLAN alias to the WLAN. The VLAN alias should to existing and configured. **Note:** A VLAN alias maps a name to a VLAN ID. When applied to ports (for example GE ports) using the trunk mode, a VLAN alias denies or permits traffic, on the port, to and from the VLANs specified in the alias. For more information on aliases, see `alias`. |

Examples

```
rfs7000-37FABE(config-wlan-test)#vlan 4
rfs7000-37FABE(config-wlan-test)#show context wlan test
ssid testWLAN1
vlan 4
bridging-mode local
encryption-type none
authentication-type none
protected-mgmt-frames mandatory
radius vlan-assignment
time-based-access days weekdays start 10:00 end 16:30
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
use aaa-policy test
use association-acl-policy test
acl exceed-rate wireless-client-denied-traffic 20 disassociate
proxy-arp-mode strict
broadcast-dhcp validate-offer
shutdown on-unadoption
http-analyze controller
rfs7000-37FABE(config-wlan-test)#
```

Related Commands

```
no
```

Removes a WLAN's default VLAN mapping
4.1.90.2.45 vlan-pool-member

wlan-mode commands

Adds a member VLAN to a WLAN's VLAN pool. Use this option to define the VLANs available to this WLAN. Additionally, define the number of wireless clients supported by each VLAN.

NOTE: Configuration of a VLAN pool overrides the 'vlan' configuration.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`vlan-pool-member <WORD> {limit <0-8192>}

Parameters

- `vlan-pool-member <WORD> {limit <0-8192>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-pool-member &lt;WORD&gt;</code></td>
<td>Adds a member VLAN to a WLAN's VLAN pool</td>
</tr>
<tr>
<td><code>limit &lt;0-8192&gt;</code></td>
<td>Define the VLANs available to this WLAN. It is either a single index, or a list of VLAN IDs (for example, 1,3,7), or a range (for example, 1-10)</td>
</tr>
<tr>
<td>Optional. Is ignored if the number of clients are limited and well within the limits of the DHCP pool on the VLAN</td>
<td></td>
</tr>
</tbody>
</table>

Examples

```
rfseg7000-37FABE(config-wlan-test)#vlan-pool-member 1-10 limit 1

rfseg7000-37FABE(config-wlan-test)#show context
wlan test
  ssid testWLAN1
  vlan-pool-member 1 limit 1
  vlan-pool-member 2 limit 1
  vlan-pool-member 3 limit 1
  vlan-pool-member 4 limit 1
  vlan-pool-member 5 limit 1
  vlan-pool-member 6 limit 1
  vlan-pool-member 7 limit 1
  vlan-pool-member 8 limit 1
  vlan-pool-member 9 limit 1
  vlan-pool-member 10 limit 1
  bridging-mode local
  encryption-type none
  authentication-type none
  protected-mgmt-frames mandatory
  radius vlan-assignment
  time-based-access days weekdays start 10:00 end 16:30
  wing-extensions wmm-load-information
  --More--
```

```
rfseg7000-37FABE(config-wlan-test)#`
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the list of VLANs mapped to a WLAN</td>
</tr>
</tbody>
</table>
4.1.90.2.46  wep128

➤ wlan-mode commands

Configures WEP128 parameters

**Supported in the following platforms:**
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`wep128 [key|keys-from-passkey|transmit-key]`

`wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]`

`wep128 keys-from-passkey <WORD>`

`wep128 transmit-key <1-4>`

**Parameters**

- **wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]**

  Configures pre-shared hex keys
  - `<1-4>` – Configures a maximum of four key indexes. Select the key index from 1 - 4.
  - **ascii**
    - `[0 <WORD>|2 <WORD>|<WORD>]` Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)
    - 0 <WORD> – Configures a clear text key
    - 2 <WORD> – Configures an encrypted key
    - <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters
  - **hex**
    - `[0 <WORD>|2 <WORD>|<WORD>]` Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128)
    - 0 <WORD> – Configures a clear text key
    - 2 <WORD> – Configures an encrypted key
    - <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters

- **wep128 keys-from-passkey <WORD>**

  Specifies a passphrase from which keys are derived
  - `<WORD>` – Specify a passphrase from 4 - 32 characters.

- **wep128 transmit-key <1-4>**

  Configures the key index used for transmission from an AP to a wireless client or service platform
  - `<1-4>` – Specify a key index from 1 - 4.
Examples
rfs7000-37FABE(config-wlan-test)#wep128 keys-from-passkey example@123
rfs7000-37FABE(config-wlan-test)#show context
wlan test
ssid testWLAN1
vlan-pool-member 1 limit 1
vlan-pool-member 2 limit 1
vlan-pool-member 3 limit 1
vlan-pool-member 4 limit 1
vlan-pool-member 5 limit 1
vlan-pool-member 6 limit 1
vlan-pool-member 7 limit 1
vlan-pool-member 8 limit 1
vlan-pool-member 9 limit 1
vlan-pool-member 10 limit 1
bridging-mode local
encryption-type none
authentication-type none
protected-mgmt-frames mandatory
wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
wep128 key 2 hex 0 2b3fb36924b22dffe98c86c315
wep128 key 3 hex 0 1ebf3394431700194762ebd5b2
wep128 key 4 hex 0 e3de75be311bd787aeac5e4e8b
radius vlan-assignment
time-based-access days weekdays start 10:00 end 16:30
--More--
rfs7000-37FABE(config-wlan-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the WEP128 PSK and transmission keys to factory-default values.</td>
</tr>
</tbody>
</table>
# 4.1.90.2.47 wep64

> **wlan-mode commands**

Configures WEP64 parameters

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

## Syntax

- `wep64 [key|keys-from-passkey|transmit-key]`
- `wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]`
- `wep64 keys-from-passkey <WORD>`
- `wep64 transmit-key <1-4>`

## Parameters

- **wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]**
  - Configures pre-shared hex keys
  - `<1-4>` – Configures a maximum of four key indexes. Select a key index from 1 - 4.
  - **ascii**
    - `[0 <WORD>|2 <WORD>|<WORD>]` – Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)
  - **hex**
    - `[0 <WORD>|2 <WORD>|<WORD>]` – Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128)
- **wep64 keys-from-passkey <WORD>**
  - Specifies a passphrase from which keys are derived
  - `<WORD>` – Specify a passphrase from 4 - 32 characters.
- **wep64 transmit-key <1-4>**
  - Configures the key index used for transmission from an AP to a wireless client or service platform
  - `<1-4>` – Specify a key index from 1 - 4.
Examples

rfs7000-37FABE(config-wlan-test)#wep64 key 1 ascii test1
rfs7000-37FABE(config-wlan-test)#wep64 transmit-key 1
rfs7000-37FABE(config-wlan-test)#show context
  wlan test
    ssid testWLAN1
    vlan-pool-member 1 limit 1
    vlan-pool-member 2 limit 1
    vlan-pool-member 3 limit 1
    vlan-pool-member 4 limit 1
    vlan-pool-member 5 limit 1
    vlan-pool-member 6 limit 1
    vlan-pool-member 7 limit 1
    vlan-pool-member 8 limit 1
    vlan-pool-member 9 limit 1
    vlan-pool-member 10 limit 1
    bridging-mode local
    encryption-type none
    authentication-type none
    protected-mgmt-frames mandatory
    wep64 key 1 hex 0 7465737431
    radius vlan-assignment
    time-based-access days weekdays start 10:00 end 16:30
    wing-extensions wmm-load-information
    client-load-balancing probe-req-intvl 5ghz 5
    client-load-balancing band-discovery-intvl 2
    use aaa-policy test
    --More--
rfs7000-37FABE(config-wlan-test)#

Related Commands

| no           | Resets the WEP64 PSK and transmission keys to factory-default values |
4.1.90.2.48 wing-extensions

4.1.90.2.48 wing-extensions

- **wlan-mode commands**

Enables support for WiNG-specific client extensions to the IEEE 802.11x WLAN standards that potentially increase client roaming reliability and handshake speed.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
wing-extensions [ap-attributes-information {include-hostname}]
coverage-hole-detection {11k-clients|offset <5-20>|threshold <-80--60}]
ft-over-ds-aggregate|move-command|scan-assist {channel-info-interval <6-9>}
smart-scan|wing-load-information|wmm-load-information]
```

**Parameters**

- **wing-extensions [ap-attributes-information {include-hostname}]
coverage-hole-detection {11k-clients|offset <5-20>|threshold <-80--60}]
ft-over-ds-aggregate|move-command|scan-assist {channel-info-interval <6-9>}
smart-scan|wing-load-information|wmm-load-information]

<table>
<thead>
<tr>
<th>wing-extensions</th>
<th>Enables support for inclusion of WiNG-specific client extensions in radio transmissions</th>
</tr>
</thead>
</table>
| ap-attributes-information {include-hostname} | Enables support for AP attributes information element (IE)
  - include-hostname – Optional. When enabled, includes AP’s hostname, as a sub-element, in the AP attributes IE. The AP attributes IE is vendor-specific and, when enabled, is added to beacons and probe responses. Inclusion of AP attributes IE allows Zebra terminals to:
    - Recognize Zebra APs
    - Determine if the AP supports PAN BU features, irrespective of whether these features are enabled or not.
  **Note:** AP attributes IE is not added to beacons and probe responses by default. |
| coverage-hole-detection {11k-clients|offset <5-20>|threshold <-80--60} | Enables coverage hole detection (CHD) and configures CHD parameters. When enabled, allows clients (MUs) to inform an access point when it experiences a coverage hole. A coverage hole is an area of poor wireless coverage not supported by a WiNG managed access point radio. Enable radio resource measurement prior to enabling CHD. For enabling radio resource measurement, see radio-resource-measurement. CHD is disabled by default. After enabling CHD, optionally configure the following parameters:
  - 11k-clients – Optional. Provides coverage hole detection to 802.11k-only-capable clients. This is a reduced set of coverage hole detection capabilities (standard 11k messages and behaviors). This option is disabled by default.
  - offset <5-20> – Optional. Configures the offset added to the threshold to obtain the access point’s signal strength (as seen by the client) considered adequate. 
    - <5-20> – Specify the offset value from 5 - 20. The default is 5.
  - threshold – Optional. Configures the access point’s signal strength threshold. When Radio Resource Measurement and CVG Hole are enabled, specify a threshold for the AP’s signal strength (as seen by the client) below which a coverage hole incident is reported by the client.
    - <-80--60> – Specify the threshold from -80 - -60 dBm. The default is -70 dBm. |
### ft-over-ds-aggregate
Enables fast-transition (FT) aggregation of action frames. When enabled, increases roaming speed by eliminating separate key exchange handshake frames with potential roam candidates. Enable fast transition to complete an initial FT over distribution system (DS) handshake with multiple roam candidates (up to 6) at once, eliminating the need to send separate FT over DS handshakes to each roam candidate. This option is disabled by default.

### move-command
Enables use of Hyper Fast Secure Roaming (HFSR) for clients on this WLAN. This feature applies only to certain client devices. This option is disabled by default.

### scan-assist {channel-info-interval <6-9>}
Enables support for scanning assist. When enabled, allows faster roams on Dynamic Frequency Selection (DFS) channels by eliminating passive scans. Clients get channel information directly from possible roam candidates. This option is disabled by default.
- channel-info-interval <6-9> – Optional. Configures the interval at which channel information is periodically retrieved from potential roam candidates without requesting scan assist.
- <6-9> – Specify the interval from 6 - 9 seconds. When enabled, the default value is 8 seconds.

### smart-scan
Enables a smart scan to refine a client's channel scans to just a few channels as opposed to all available channels. This option is disabled by default.

### wing-load-information
Enables support for the WiNG load information element (Element ID 173) with legacy Symbol Technology clients, thus making them optimally interoperable with the latest Zebra access points. This option is enabled by default.

### wmm-load-information
Enables support for WiNG Wi-Fi MultiMedia (WMM) Load Information Element in radio transmissions with legacy clients. This option is disabled by default.

### Examples
```bash
rfs7000-37FABE(config-wlan-test)#wing-extensions wmm-load-information
```
```bash
rfs7000-37FABE(config-wlan-test)#show context wlan test
description TestWLAN ssid test bridging-mode local encryption-type tkip-ccmp authentication-type eap kerberos server timeout 12 kerberos server primary host 172.16.10.2 accounting syslog host 172.16.10.4 port 2 data-rates 2.4GHz gn wing-extensions wmm-load-information client-load-balancing probe-req-intvl 5ghz 5
--More--
rfs7000-37FABE(config-wlan-test)#
```

### Related Commands
- `no`
  Disables support for WiNG-specific client extensions to the IEEE 802.11x WLAN standards. Use the keywords provided to disable a specific wing-extension.
4.1.90.2.49 wireless-client

- wlan-mode commands

Configures the transmit power indicated to clients

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
wireless-client [count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|max-firewall-sessions|reauthentication|t5-inactivity-timeout|tx-power|vlan-cache-ageout]

wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|hold-time <1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|reauthentication <30-86400>|t5-inactivity-timeout <60-86400>|tx-power <0-20>|vlan-cache-ageout <60-86400>]

wireless-client roam-notification [after-association|after-data-ready|auto]

Parameters
- wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|hold-time <1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|reauthentication <30-86400>|t5-inactivity-timeout <60-86400>|tx-power <0-20>|vlan-cache-ageout <60-86400>]

<table>
<thead>
<tr>
<th>wireless-client</th>
<th>Configures the transmit power indicated to wireless clients for transmission</th>
</tr>
</thead>
</table>
| count-per-radio <0-256> | Configures the maximum number of clients allowed on this WLAN per radio  
  • <0-256> – Specify a value from 0 - 256. |
| cred-cache-ageout <60-86400> | Configures the timeout period for which client credentials are cached across associations  
  • <60-86400> – Specify a value from 60 - 86400 seconds. |
| hold-time <1-86400> | Configures the time period for which wireless client state information is cached post roaming  
  • <1-86400> – Specify a value from 1 - 86400 seconds. |
| inactivity-timeout <60-86400> | Configures an inactivity timeout period in seconds. If a frame is not received from a wireless client for this period of time, the client is disassociated.  
  • <60-86400> – Specify a value from 60 - 86400 seconds. |
| max-firewall-sessions <10-10000> | Configures the maximum firewall sessions allowed per client on a WLAN  
  • <10-10000> – Specify the maximum number of firewall sessions allowed from 10 - 10000. |
| reauthentication <30-86400> | Configures periodic reauthentication of associated clients  
  • <30-86400> – Specify the client reauthentication interval from 30 - 86400 seconds. |
| t5-inactivity-timeout <60-86400> | Configures an inactivity timeout, in seconds, for T5 devices. When configured, the T5 device is disassociated if the time lapsed after the last frame received from it exceeds the value specified here.  
  • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 60 seconds. |
tx-power <0-20>  Configures the transmit power indicated to clients
•  <0-20> – Specify a value from 0 - 20 dBm.

vlan-cache-ageout <60-86400>  Configures the timeout period for which client VLAN information is cached across associations.
•  <60-86400> – Specify a value from 60 - 86400 seconds.

• wireless-client roam-notification [after-association|after-data-ready|auto]

wireless-client Configures the transmit power indicated to wireless clients for transmission
roam-notification Configures when a roam notification is transmitted
after-association Transmits a roam notification after a client has associated
after-data-ready Transmits a roam notification after a client is data-ready (after completion of authentication, handshakes etc.)
auto Transmits a roam notification upon client association (if the client is known to have authenticated to the network)

Examples
rfs7000-37FABE(config-wlan-test)#wireless-client cred-cache-ageout 65
rfs7000-37FABE(config-wlan-test)#wireless-client hold-time 200
rfs7000-37FABE(config-wlan-test)#wireless-client max-firewall-sessions 100
rfs7000-37FABE(config-wlan-test)#wireless-client reauthentication 35
rfs7000-37FABE(config-wlan-test)#wireless-client tx-power 12
rfs7000-37FABE(config-wlan-test)#show context
wlan test
  ssid testWLAN1
  vlan-pool-member 1 limit 1
  vlan-pool-member 2 limit 1
  vlan-pool-member 3 limit 1
  vlan-pool-member 4 limit 1
  vlan-pool-member 5 limit 1
  vlan-pool-member 6 limit 1
  vlan-pool-member 7 limit 1
  vlan-pool-member 8 limit 1
  vlan-pool-member 9 limit 1
  vlan-pool-member 10 limit 1
  bridging-mode local
  encryption-type none
  authentication-type none
  wireless-client hold-time 200
  wireless-client cred-cache-ageout 65
  wireless-client max-firewall-sessions 100
  protected-mgmt-frames mandatory
  wireless-client reauthentication 35
  time-based-access days weekdays start 10:00 end 16:30
  wing-extensions wmm-load-information
  wireless-client tx-power 12
  client-load-balancing probe-req-intvl 5ghz 5
  --More--
rfs7000-37FABE(config-wlan-test)#
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes or reverts to default configured wireless client related parameters</td>
</tr>
</tbody>
</table>
4.1.90.2.50  wpa-wpa2


### wlan-mode commands

Modifies TKIP-CCMP (WPA/WPA2) related parameters

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```plaintext
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|server-only-authentication|psk|tkip-countermeasures|use-sha256-akm]
```

```plaintext
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|server-only-authentication|use-sha256-akm]
```

```plaintext
wpa-wpa2 handshake [attempts|init-wait|priority|timeout]
```

```plaintext
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]|timeout <10-5000> [10-5000]]
```

```plaintext
wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>
```

```plaintext
wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]
```

```plaintext
wpa-wpa2 tkip-countermeasures holdtime <0-65535>
```

### Parameters

- **wpa-wpa2** [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|server-only-authentication|use-sha256-akm]

- **wpa-wpa2 handshake** [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]|timeout <10-5000> [10-5000]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude-wpa2-tkip</td>
<td>Excludes the Wi-Fi Protected Access II (WPA2) version of TKIP. It supports the WPA version of TKIP only. This option is disabled by default.</td>
</tr>
<tr>
<td>opp-pmk-caching</td>
<td>Uses opportunistic key caching (same Pairwise Master Key (PMK) across APs for fast roaming with EAP.802.1x. This option is enabled by default.</td>
</tr>
<tr>
<td>pmk-caching</td>
<td>Uses cached pair-wise master keys (fast roaming with eap/802.1x). This option is enabled by default.</td>
</tr>
<tr>
<td>preauthentication</td>
<td>Uses pre-authentication mode (WPA2 fast roaming)</td>
</tr>
<tr>
<td>server-only-authentication</td>
<td>Uses online sign up server-only-authenticated encryption network. This option is disabled by default.</td>
</tr>
<tr>
<td>use-sha256-akm</td>
<td>Uses sha256 authentication key management suite. This option is disabled by default.</td>
</tr>
</tbody>
</table>

- **wpa-wpa2 handshake** [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]|timeout <10-5000> [10-5000]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attempts &lt;1-5&gt;</td>
<td>Configures the total number of times a message is transmitted towards a non-responsive client</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-5&gt; – Specify a value from 1 - 5. The default is 2.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>init-wait</td>
<td>Configures a minimum wait-time period, in microseconds, before the first handshake message is transmitted from the AP. This option is disabled by default.</td>
</tr>
<tr>
<td>&lt;5-1000000&gt;</td>
<td>• &lt;5-1000000&gt; – Specify a value from 5 - 1000000 microseconds.</td>
</tr>
<tr>
<td>priority [high</td>
<td>normal]</td>
</tr>
<tr>
<td></td>
<td>• high – Treats handshake messages as high priority packets on a radio. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• normal – Treats handshake messages as normal priority packets on a radio</td>
</tr>
<tr>
<td>timeout &lt;10-5000&gt;</td>
<td>Configures the timeout period, in milliseconds, for a handshake message to retire. Once this period is exceed, the handshake message is retired.</td>
</tr>
<tr>
<td>&lt;10-5000&gt;</td>
<td>• &lt;10-5000&gt; – Specify a value from 10 - 5000 milliseconds. The default is 500 milliseconds.</td>
</tr>
<tr>
<td>wpa-wpa2 key-rotation [broadcast</td>
<td>unicast] &lt;30-86400&gt;</td>
</tr>
<tr>
<td>wpa-wpa2</td>
<td>Modifies TKIP-CCMP (WPA/WPA2) related parameters</td>
</tr>
<tr>
<td>key-rotation</td>
<td>Configures the periodic rotation of keys used for broadcast and multicast traffic. This parameter specifies the interval, in seconds, at which keys are rotated. This option is disabled by default.</td>
</tr>
<tr>
<td>broadcast &lt;30-86400&gt;</td>
<td>• &lt;30-86400&gt; – Specify a value from 30 - 86400 seconds.</td>
</tr>
<tr>
<td>unicast &lt;30-86400&gt;</td>
<td>Configures a periodic interval for the rotation of keys, used for unicast traffic. This option is disabled by default.</td>
</tr>
<tr>
<td>wpa-wpa2 psk [0 &lt;LINE&gt;</td>
<td>2 &lt;LINE&gt;</td>
</tr>
<tr>
<td>wpa-wpa2 psk</td>
<td>Modifies TKIP-CCMP (WPA/WPA2) related parameters</td>
</tr>
<tr>
<td>0 &lt;LINE&gt;</td>
<td>Configures a clear text key</td>
</tr>
<tr>
<td>2 &lt;LINE&gt;</td>
<td>Configures an encrypted key</td>
</tr>
<tr>
<td>&lt;LINE&gt;</td>
<td>Enter the pre-shared key either as a passphrase not exceeding 8 - 63 characters, or as a 64 character (256bit) hexadecimal value</td>
</tr>
<tr>
<td>wpa-wpa2 tkip-countermeasures holdtime &lt;0-65535&gt;</td>
<td>Configures a hold time period for implementation of TKIP counter measures</td>
</tr>
<tr>
<td>wpa-wpa2</td>
<td>Modifies TKIP-CCMP (WPA/WPA2) parameters</td>
</tr>
<tr>
<td>tkip-countermeasures</td>
<td>Configures the amount of time a WLAN is disabled when TKIP counter measures are invoked</td>
</tr>
<tr>
<td>holdtime &lt;0-65535&gt;</td>
<td>• &lt;0-65535&gt; – Specify a value from 0 - 65535 seconds. The default is 60 seconds.</td>
</tr>
</tbody>
</table>
Examples
rfs7000-37FABE(config-wlan-test)#wpa-wpa2 tkip-countermeasures hold-time 2
rfs7000-37FABE(config-wlan-test)#show context wlan test
ssid testWLAN1
tag testWLAN
vlan-pool-member 1 limit 1
vlan-pool-member 2 limit 1
vlan-pool-member 3 limit 1
vlan-pool-member 4 limit 1
vlan-pool-member 5 limit 1
vlan-pool-member 6 limit 1
vlan-pool-member 7 limit 1
vlan-pool-member 8 limit 1
vlan-pool-member 9 limit 1
vlan-pool-member 10 limit 1
bridging-mode local
encryption-type none
authentication-type none
wireless-client hold-time 200
wireless-client cred-cache-ageout 65
wireless-client max-firewall-sessions 100
protected-mgmt-frames mandatory
wireless-client reauthentication 35
wpa-wpa2 tkip-countermeasures hold-time 2
wep64 key 1 hex 0 7465737431
wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
--More--
rfs7000-37FABE(config-wlan-test)#

Related Commands

| no | Removes or reverts to default TKIP-CCMP (WPA/WPA2) related parameters |
**4.1.90.2.51 service**

Invokes service commands applicable in the WLAN configuration mode

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
service [allow-ht-only|allow-open-passpoint|cred-cache|eap-mac-mode|eap-mac-multicopy|
eap-mac-multikeys|eap-throttle|enforce-pmkid-validation|key-index|monitor|
radio-crypto|reauthentication|session-timeout|session-timeout mac|tx-deauth-on-roam-detection|
unresponsive-client|wpa-wpa2|show]

service [allow-ht-only|allow-open-passpoint|cred-cache clear-on-disconnect|
eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-validation|radio-crypto|
reauthentication seamless|session-timeout mac|tx-deauth-on-roam-detection|show cli]

service eap-mac-mode [mac-always|normal]

service eap-throttle <0-254>

service key-index eap-wep-unicast <1-4>

service monitor [aaa-server|adoption|captive-portal|dhcp|dns]

service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]

service [dhcp|dns] crm <RESOURCE-NAME> vlan <1-4094>

service unresponsive-client [attempts <1-1000>|timeout <1-60>]

service wpa-wpa2 exclude-ccmp
```

**Parameters**

- `allow-ht-only`: Only allows clients capable of High Throughput (802.11n) data rates to associate
- `allow-open-passpoint`: Enables non-WPA2 security for passpoint WLANs. For more information on passpoint policy and configuration, see PASSPOINT POLICY.
- `cred-cache clear-on-disconnect`: Clears credential cache after a client has disconnected from the network
- `eap-mac-multicopy`: Enables sending of multiple copies of broadcast and unicast messages
- `eap-mac-multikeys`: Enables configuration of different key indices for MAC authentication
- `enforce-pmkid-validation`: Validates the Predictive real-time pairwise master key identifier (PMKID) contained in a client’s association request against the one present in the wpa-wpa2 handshake. This functionality is based on the Proactive Key Caching (PKC) extension of the 802.11i EEEE standard. Whenever a wireless client successfully authenticates with a AP it receives a pairwise master key (PMK). PKC allows clients to cache this PMK and reuse it for future re-authentications with the same AP. The PMK is unique for every client and is identified by the PMKID. The PMKID is a combination of the hash of the PMK, a string, the station and the MAC addresses of the AP.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio-crypto</td>
<td>Uses radio hardware for encryption and decryption. This is applicable only for devices using <em>Counter Cipher Mode with Block Chaining Message Authentication Code Protocol</em> (CCMP) encryption mode.</td>
</tr>
<tr>
<td>reauthentication</td>
<td>Enables seamless EAP client reauthentication without disconnecting client after the session has timed out</td>
</tr>
<tr>
<td>session-timeout mac</td>
<td>Enables reauthentication of MAC authenticated clients without disconnecting client after the session has timed out</td>
</tr>
<tr>
<td>tx-deauth-on-roam-detection</td>
<td>Transmits a deauthentication on the air while disassociating a client because its roam is detected on the wired side</td>
</tr>
<tr>
<td>show cli</td>
<td>Displays the CLI tree of the current mode. When used in the WLAN mode, this command displays the WLAN CLI structure.</td>
</tr>
</tbody>
</table>

- **service eap-mac-mode [mac-always|normal]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap-mac-mode</td>
<td>Configures the EAP and/or MAC authentication mode used with this WLAN</td>
</tr>
<tr>
<td>mac-always</td>
<td>Enables both EAP and MAC authentication. MAC authentication is performed first, followed by EAP authentication. Clients are granted access based on the EAP authentication result. If a client does not have EAP, the MAC authentication result is used to grant access.</td>
</tr>
<tr>
<td>normal</td>
<td>Grants client access if the client clears either EAP or MAC authentication</td>
</tr>
</tbody>
</table>

- **service eap-throttle <0-254>**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap-throttle</td>
<td>Enables EAP request throttling. Use this command to specify the maximum number of parallel EAP sessions allowed on this WLAN. Once this specified value is exceeded, all incoming EAP session requests are throttled.</td>
</tr>
<tr>
<td>• &lt;0-254&gt; – Specify a value from 0 - 254.</td>
<td></td>
</tr>
</tbody>
</table>

- **service key-index eap-wep-unicast <1-4>**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-index eap-wep-unicast</td>
<td>Configures an index with each key during EAP authentication with WEP</td>
</tr>
<tr>
<td>• &lt;1-4&gt; – Select a index from 1 - 4.</td>
<td></td>
</tr>
</tbody>
</table>

- **service wpa-wpa2 exclude-ccmp**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wpa-wpa2 exclude-ccmp</td>
<td>Configures exclusion of CCMP requests when the authentication mode is set to tkip-ccmp. When enabled, it provides compatibility for client devices not compliant with tkip-ccmp.</td>
</tr>
</tbody>
</table>

- **service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Enables critical resource monitoring. In a WLAN, service monitoring enables regular monitoring of external AAA servers, captive portal servers, access point adoption, DHCP and DNS servers. When enabled, it allows administrators to notify users of a service’s availability and make resource substitutions in case of unavailability of a service.</td>
</tr>
<tr>
<td>aaa-server</td>
<td>Enables external AAA server failure monitoring. When enabled monitors an external RADIUS server resource’s AAA activity and ensures its adoption and availability. This feature is disabled by default.</td>
</tr>
</tbody>
</table>
adoption_vlan <1-4094>

Enables adoption failure monitoring on an adopted AP. Also configures a adoption failover VLAN. This feature is disabled by default.

- **VLAN <1-4094>** – Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost.

**Note:** Configure a DHCP pool and gateway for the failover VLAN. Ensure the DHCP server is running on the AP. Also ensure that the DHCP pool is configured to have less lease time.

When this feature is enabled on a WLAN, it allows adopted APs to monitor their connectivity with the controller. If and when this connectivity is lost, all new clients are placed in the configured adoption failover VLAN. They are served an IP by the DHCP server running on the AP. In this situation if a client tries to access a Web URL, the AP redirects the client to a page stating that the service is down.

**Note:** When the AAP’s link to the switch is restored, clients are placed back in the WLAN’s configured VLAN, and are served an IP from the corresponding configured DHCP server (external or on the AP/controller).

captive-portal

enables external captive portal server failure monitoring. When enabled, monitors externally hosted captive portal activity, and user access to the controller or service platform managed network. This feature is disabled by default.

**Note:** When enabled, this feature enables APs to display, to an externally located captive portal's user, the no-service page when the captive portal's server is not reachable.

```
• service monitor [dhcp|dns] crm <RESOURCE-NAME> vlan <1-4094>]
```

monitor Enables DHCP and/or DNS server monitoring on this WLAN.

dhcp Enables monitoring of a specified DHCP server. When the connection to the DHCP server is lost, captive portal users automatically migrate to a pre-defined VLAN. The feature is disabled by default.

**Note:** Use the `crm` keyword to specify the DHCP server to monitor.

dns Enables monitoring of a specified DNS server. When the connection to the DNS server is lost, captive portal users automatically migrate to a pre-defined VLAN. The feature is disabled by default.

**Note:** Use the `crm` keyword to specify the DNS server to monitor.

crm <RESOURCE-NAME>

This keyword is common to the ‘dhcp’ and ‘dns’ parameters.

- **crm** – Identifies the DHCP and/or DNS server to monitor
- **<RESOURCE-NAME>** – Specify the name of the DHCP or DNS server.

**Note:** Once enabled, the CRM server monitors the DHCP/DNS server and updates their status as ‘up’ or ‘down’ depending on the availability of the resource. When either of these resources is down the wireless client is mapped to the failover VLAN and served with the ‘no-service’ page through the access point.

vlan <1-4094>

This keyword is common to the ‘dhcp’ and ‘dns’ parameters.

After specifying the DHCP/DNS sever resource, specify the failover VLAN.

- **VLAN <1-4094>** – Configures the failover VLAN from 1 - 4094.

**Note:** When the DHCP server resource becomes unavailable, the device falls back to the VLAN defined here. This VLAN has a DHCP server configured that provides a pool of IP addresses with a lease time less than the main DHCP server.

**Note:** When this DNS server resource becomes unavailable, the device falls back to the VLAN defined here. This VLAN has a DNS server configured that provides DNS address resolution until the main DNS server becomes available.
• service unresponsive-client [attempts <1-1000>|timeout <1-60>]

<table>
<thead>
<tr>
<th>eap-mac-mode</th>
<th>Configures handling of unresponsive clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>attempts &lt;1-1000&gt;</td>
<td>Configures the maximum number of successive packets that failed transmission</td>
</tr>
<tr>
<td>• &lt;1-1000&gt; – Specify a value from 1 - 1000.</td>
<td></td>
</tr>
<tr>
<td>timeout &lt;1-60&gt;</td>
<td>Configures the interval, in seconds, for successive packets not acknowledged by the client</td>
</tr>
<tr>
<td>• &lt;1-60&gt; – Specify a value from 1 - 60 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58(config-wlan-test)#service allow-ht-only
rfs4000-229D58(config-wlan-test)#service monitor aaa-server
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 service monitor aaa-server
 service allow-HT-only
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#

Related Commands

| no | Removes or reverts to default WLAN settings configured using the ‘service’ command |
**4.1.91 wlan-qos-policy**

> **Global Configuration Commands**

Configures a WLAN QoS policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wlan-qos-policy <WLAN-QOS-POLICY-NAME>
```

**Parameters**

- `wlan-qos-policy <WLAN-QOS-POLICY-NAME>`

**Examples**

```
rfs7000-37FABE(config)#wlan-qos-policy test
rfs7000-37FABE(config-wlan-qos-test)#?
```

**WLAN QoS Mode commands:**

- `accelerated-multicast`: Configure accelerated multicast streams address assnd forwarding QoS classification
- `classification`: Select how traffic on this WLAN must be classified (relative prioritization on the radio)
- `multicast-mask`: Egress multicast mask (frames that match bypass the PSPqueue. This permits intercom mode operation without delay even in the presence of PSP clients)
- `no`: Negate a command or set its defaults
- `qos`: Quality of service
- `rate-limit`: Configure traffic rate-limiting parameters on a per-wlan/per-client basis
- `svp-prioritization`: Enable spectralink voice protocol support on this wlan
- `voice-prioritization`: Prioritize voice client over other client (for non-WMM clients)
- `wmm`: Configure 802.11e/Wireless MultiMedia parameters

```
clrscr
commit
do
end
exit
help
revert
service
show
write
```

```
rfs7000-37FABE(config-wlan-qos-test)#
```

---

**NOTE:** For more information on WLAN QoS policy commands, see *Chapter 21, WLAN-QOS-POLICY*. 
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an existing WLAN QoS Policy</td>
</tr>
</tbody>
</table>
4.1.92 smart-cache-policy

The following table lists the smart cache policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>smart-cache-policy</td>
<td>Creates a new smart cache policy and enters its configuration mode</td>
<td>page 4-450</td>
</tr>
<tr>
<td>smart-cache-policy-mode commands</td>
<td>Summarizes the smart cache policy configuration mode commands</td>
<td>page 4-452</td>
</tr>
</tbody>
</table>
4.1.92.1 smart-cache-policy

Creates a new smart cache policy and enters its configuration mode.

Content caching is a mechanism that allows temporary caching of frequently accessed content on intermediate network devices. When enabled, subsequent requests for the same content are serviced from the cache locally and not fetched from originating servers, resulting in reduced bandwidth usage, lower latency, and reduced data transfers from originating servers. The WiNG smart cache policy supports both forward caching and transparent caching.

Forward content caching stores content temporarily on the local network. This locally stored content can be retrieved, when required, without routing a request to an external server on the Internet.

Transparent content caching, on the other hand, acts as an intermediary for the originating servers and returns cached content to clients as if the data originated from the associated servers. Transparent caching proxies perform server load-balancing and compression to regulate load on the originating servers and reduce bandwidth usage.

The smart cache policy also supports dynamic content caching, allowing caching of content from popular video content sharing sites, such as youtube.com, cnn.com, msn.com etc.

Enabling content caching improves Web browsing (for data and video content) for consumers using Kiosks, tablets, and smart phones. A smart cache policy is enabled by associating it with a device or a profile.

Configure the policy’s forward proxy, transparent proxy and several additional settings before actual HTML pages can be defined for the smart caching configuration.

### Syntax

```
smart-cache-policy <SMART-CACHE-POLICY-NAME>
```

### Parameters

- `smart-cache-policy <SMART-CACHE-POLICY-NAME>`

### Examples

```
nx4500-5CFA2B(config)#smart-cache-policy ?
SMART-CACHE-POLICY Name of the content caching to be configured ( will be created if it does not exist )
```

```
nx4500-5CFA2B(config)#smart-cache-policy test
nx4500-5CFA2B(config-smart-cache-policy-test)#
```
nx4500-5CFA2B(config-smart-cache-policy-test)#?
Content Cache Policy Mode commands:
  access-log Log all client requests
  aging Configure the refresh pattern
  cache Configure cache management
  forward-proxy Configure address and port for forward caching proxy
  http-access Configure http filter
  no Negate a command or set its defaults
  parent-proxy Configure parent proxy
  pre-fetch Enable pre-fetching of a URL list
  smart-cache Content cache
  transparent-proxy Transparent caching proxy
  clrscr Clears the display screen
  commit Commit all changes made in this session
  do Run commands from Exec mode
  end End current mode and change to EXEC mode
  exit End current mode and down to previous mode
  help Description of the interactive help system
  revert Revert changes
  service Service Commands
  show Show running system information
  write Write running configuration to memory or terminal

nx4500-5CFA2B(config-smart-cache-policy-test)#
4.1.92.2 smart-cache-policy-mode commands

The following table summarizes smart cache policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-log</td>
<td>Enables client request logging</td>
<td>page 4-453</td>
</tr>
<tr>
<td>aging</td>
<td>Configures the refresh pattern (aging parameters) for specific content types</td>
<td>page 4-454</td>
</tr>
<tr>
<td>cache</td>
<td>Configures cache management settings</td>
<td>page 4-456</td>
</tr>
<tr>
<td>forward-proxy</td>
<td>Configures the address and port for forward caching proxy service</td>
<td>page 4-458</td>
</tr>
<tr>
<td>http-access</td>
<td>Configures HTTP filters – access control lists (ACLs)</td>
<td>page 4-460</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets content cache policy settings</td>
<td>page 4-462</td>
</tr>
<tr>
<td>pre-fetch</td>
<td>Enables pre fetching of URL lists</td>
<td>page 4-463</td>
</tr>
<tr>
<td>parent-proxy</td>
<td>Enables parent proxy on this smart cache policy</td>
<td>page 4-464</td>
</tr>
<tr>
<td>smart-cache</td>
<td>Enables smart content caching</td>
<td>page 4-465</td>
</tr>
<tr>
<td>transparent-proxy</td>
<td>Configures transparent caching proxy settings</td>
<td>page 4-466</td>
</tr>
</tbody>
</table>
4.1.92.2.1 access-log

*smart-cache-policy-mode commands*

Enables client request logging. When enabled, this feature logs client access details to the /var/log/smart-cache.log. This feature is enabled by default.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`access-log {rotate <0-10> rotate-type [duration <1-100> day|size <1-100> MB]}

**Parameters**

- `access-log {rotate <0-10> rotate-type [duration <1-100> day|size <1-100> MB]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| rotate <0-10>      | Optional. Enables log file rotation, and configures the number of rotation. This is the number of log files retained (stored locally) out of the total generated.  
  - <0-10> – Optional. Specify the number of rotations from 0 - 10. The default is 10 rotations on every 1 MB. |
| rotate-type [duration <1-100> day|size <1-100> MB] | Optional. Configures access log file rotation conditions, such as duration and size  
  - duration <1-100> – Rotates log files by time. Specify the time from 1 - 100 days. The default is 1 day.  
  - size <1-100> – Rotates log files by file size. Specify the size from 1 - 100 MB. |

**Examples**

`nx4500-5CFA2B(config-smart-cache-policy-test)#access-log rotate 10 rotate-type duration 10 day`

`nx4500-5CFA2B(config-smart-cache-policy-test)#show context smart-cache-policy test
  access-log rotate 10 rotate-type duration 10 day`

**Related Commands**

- `no` Disables client request logging
4.1.92.2.2 aging

* smart-cache-policy-mode commands

Configures the aging rule (refresh pattern) for specific content types

The aging parameters configured are the maximum and minimum age, freshness factor, and the URL regular expressions. These parameters enable the content caching engine to determine if a given request can be processed and the content loaded from the cache or not.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
aging precedence <1-100> [<WORD>|ignore-case <WORD>] min-age <0-525600>
  freshness-factor <0-100> max-age <0-525600> {(override-expire|override-lastmod|
  reload-into-ims)}
```

**Parameters**

- **aging precedence <1-100> [<WORD>|ignore-case <WORD>] min-age <0-525600>**
  - **freshness-factor <0-100> max-age <0-525600>**
  - `{(override-expire|override-lastmod|reload-into-ims)}`

<table>
<thead>
<tr>
<th>aging precedence &lt;1-100&gt;</th>
<th>Configures content cache aging rules and assigns a precedence to each rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>Specifies the regular expression to match. This option is case sensitive, and is the default setting.</td>
</tr>
<tr>
<td>ignore-case &lt;WORD&gt;</td>
<td>Specifies the regular expression to match. This option is not case sensitive.</td>
</tr>
<tr>
<td>min-age &lt;0-525600&gt;</td>
<td>Configures the minimum age, in minutes, of matched objects. This value specifies the lower limit on the staleness of a response. A response is not considered stale unless its time in the cache exceeds the specified minimum value.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-525600&gt; – Specify a value from 0 - 525600 minutes. The default is 1 minute.</td>
</tr>
<tr>
<td>freshness-factor &lt;0-100&gt;</td>
<td>Configures the freshness factor of matched objects as a percentage value. Freshness is an expression of how long Web content resides on the service platform's local cache before being updated or removed.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-100&gt; – Specify a value from 0 - 100%. The default is 100%.</td>
</tr>
<tr>
<td>max-age &lt;0-525600&gt;</td>
<td>Configures the maximum age, in minutes, of matched objects. This value specifies the upper limit on the freshness of a response. A response is not considered fresh unless its time in the cache is less than the specified maximum value.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-525600&gt; – Specify a value from 0 - 525600 minutes. The default is 525600.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes an existing aging rule (refresh pattern)</td>
</tr>
</tbody>
</table>
4.1.92.2.3  cache

smart-cache-policy-mode commands

Configures cache management settings

This command specifies content cache rules that determine if a content is cached or not. Use this feature to filter content before caching. By default content is not cached.

Supported in the following platforms:
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`cache [media|precedence|size]`

`cache media {all|aol|bing|break|cnn|daily-motion|metacafe|vimeo|youtube}`

`cache precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|destination-domain-regex <WORD>|destination-ip [<IP/M]|any]|source-ip <IP/M>|url-regex <URL>}`

`cache size <1-32>`

Parameters
• cache media {all|aol|bing|break|cnn|daily-motion|metacafe|vimeo|youtube}

<table>
<thead>
<tr>
<th>cache media</th>
<th>Enables content caching from the following video content sharing sites. The sites currently supported are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>aol.com</td>
<td></td>
</tr>
<tr>
<td>bing.com</td>
<td></td>
</tr>
<tr>
<td>break.com</td>
<td></td>
</tr>
<tr>
<td>dailymotion.com</td>
<td></td>
</tr>
<tr>
<td>metacafe.com</td>
<td></td>
</tr>
<tr>
<td>vimeo.com</td>
<td></td>
</tr>
<tr>
<td>cnn.com</td>
<td></td>
</tr>
<tr>
<td>youtube.com</td>
<td></td>
</tr>
<tr>
<td>Note: Select All to include the entire list of supported sites. Selected sites have their video content cached locally on the service platform and made available to clients that request the video content.</td>
<td></td>
</tr>
</tbody>
</table>

• cache precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|destination-domain-regex <WORD>|destination-ip [<IP/M]|any]|source-ip <IP/M>|url-regex <URL>}

<table>
<thead>
<tr>
<th>cache precedence &lt;1-100&gt;</th>
<th>Configures cache filtering rules that determine if a content received from the originating server is to be cached or not. You can create multiple cache filtering rules and assign precedence values to each. These rules are applied in order of their precedence.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[deny</td>
<td>permit]</td>
</tr>
</tbody>
</table>

| [deny|permit] | Configures the deny or permit caching parameters for this rule |
| --- | --- |
| permits – Caches content if it matches the defined permit parameters | |
| deny – Does not cache content if it matches the defined deny parameters | |
### Global Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| `cache size <1-32>`   | Configures the maximum caching storage size. This is the upper limit on the disk space used for storing cached contents.  
  • `<1-32>` – Specify a value from 1 - 32 GB. The default is 32 GB. | nx4500-5CFA2B(config-smart-cache-policy-test)#cache size 30  
  nx4500-5CFA2B(config-smart-cache-policy-test)#show context  
  smart-cache-policy test  
  cache size 30  
  aging precedence 1 ignore-case \.jpg$ min-age 100 freshness-factor 75 max-age 200  
  reload-into-ims  
  access-log rotate 10 rotate-type duration 10 day  
  nx4500-5CFA2B(config-smart-cache-policy-test)# |
| `no`                  | Resets or removes cache management settings                                                            |                                                                         |

#### Related Commands

- `destination-domain <DOMAIN-NAME>`: Optional. Specifies the destination domain's hostname to match. The domain name can be an FQDN. The specified value is matched against the hostname part of the HTTP request URL.  
  - `<DOMAIN-NAME>` – Specify the domain name.  
  A leading asterisk or period in the domain name is treated as a wildcard. For example, `www.example-company.com`, `example-company.com`, `*.example-company.com` and `.com` are all valid values.  
  **Note:** The destination domain parameter will NOT match against URLs that have an IP address instead of a hostname.  

- `destination-domain-regex <WORD>`: Optional. Specifies a regular expression matching on originating server names.  
  • `<WORD>` – Specify the regular expression.  
  The destination domain regex is the same as the destination domain, but the destination domain regex allows you to use standard expression matching on originating server names.  

- `destination-ip [<IP/M>|any]`: Optional. Specifies the originating server's IP address, obtained from the HTTP request URL.  
  • `<IP/M>` – Specify the destination IP address and mask to match.  
  • `any` – Select to specify any destination IP address as the match criteria.  
  **Note:** Provide the IP address in the A.B.C.D/M format.  
  **Note:** Specify `any` to consider all originating servers.  

- `source-ip [<IP/M>|any]`: Optional. Specifies the source IP address (client's IP address) that is sent out as part of the HTTP request.  
  • `<IP/M>` – Specify the source IP address and mask to match.  
  • `any` – Select to specify any source IP address as the match criteria.  
  **Note:** Provide the IP address in the A.B.C.D/M format.  
  **Note:** Specify `any` to consider all client requests.  

- `url-regex <URL>`: Optional. Specifies regular expressions used to match any part of a requested URL, including the transfer protocol and origin server hostname.  
  • `<URL>` – Specify the regular expression to match.  

---

**Examples**

nx4500-5CFA2B(config-smart-cache-policy-test)#cache size 30  
xx4500-5CFA2B(config-smart-cache-policy-test)#show context  
smart-cache-policy test  
    cache size 30  
    aging precedence 1 ignore-case \.jpg$ min-age 100 freshness-factor 75 max-age 200  
    reload-into-ims  
    access-log rotate 10 rotate-type duration 10 day  
xx4500-5CFA2B(config-smart-cache-policy-test)#
4.1.92.2.4 forward-proxy

smart-cache-policy-mode commands

Enables forward proxy mode on this smart cache policy. This option is disabled by default. Devices using this smart-cache policy act as a forward proxy on specified VLANs.

This command configures the IP address and port on which the forward proxy server listens for incoming HTTP requests.

Forward content caching stores content temporarily on the local network. This locally stored content can be retrieved, when required, without routing a request to an external server on the Internet.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

forward-proxy {ip|protocol|vlan}

forward-proxy {ip <IP> port <1-32768>}

forward-proxy {protocol [all|ftp|gopher|https]}

forward-proxy {vlan <VLAN-ID>}

Parameters

- forward-proxy {ip <IP> port <1-32768>}

| ip <IP> port <1-32768> | Optional. Configures the IP address and TCP port for forward proxying. If no IP address is provided, the system uses the default smart caching proxy server’s IP (127.0.1.1). This is the IP address where the forward smart caching proxy server is listening. The default port is 3128. |

- protocol [all|ftp|gopher|https]

  Optional. Selects the additional forward proxy resource protocol for smart caching. The options are:
  - ftp – Selects FTP as the forward proxy resource protocol
  - gopher – Selects Gopher as the forward proxy resource protocol
  - https – Selects HTTPS as the forward proxy resource protocol
  - all – Selects all protocols (this is the default setting)

- vlan <VLAN-ID>

  Optional. Configures the VLAN(s) for which forward proxy mode (content caching) is enabled. By default content caching is disabled on all VLANs. This option is disabled by default.

Examples

nx4500-5CFA2B(config-smart-cache-policy-test)#forward-proxy vlan 10-20

nx4500-5CFA2B(config-smart-cache-policy-test)#show context smart-cache-policy test
  forward-proxy vlan 10-20
  cache size 30
  aging precedence 1 ignore-case \\ .jgp$ min-age 100 freshness-factor 75 max-age 200
  reload-into-ims
  access-log rotate 10 rotate-type duration 10 day
  nx4500-5CFA2B(config-smart-cache-policy-test)#
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reverts address and port for forward caching proxy service</td>
</tr>
</tbody>
</table>
4.1.92.2.5 **http-access**

*smart-cache-policy-mode commands*

Configures HTTP filters. This command configures rules to deny or permit HTTP access. A deny rule specifies the destination domains and source and destination IPs to deny content access. A permit rule specifies the destination domains and source and destination IPs to permit content access.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
http-access precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|
  destination-domain-regex <WORD>|destination-ip <IP/M>|mimetype-regex <WORD>|
  source-ip <IP/M>|url-regex <URL>}
```

**Parameters**

- **http-access precedence <1-100> [deny|permit]**
  - **[deny|permit]** Configures the deny or permit access parameters for this rule
    - permits – Permits access if the specified parameters are matched
    - deny – Denies access if the specified parameters are matched

- **destination-domain <DOMAIN-NAME>**
  - Optional. Specifies the destination domain to match against the hostname in the HTTP request URL
    - <DOMAIN-NAME> – Specify the domain name.

- **destination-domain-regex <WORD>**
  - Optional. Specifies a regular expression matching on originating server names
    - <WORD> – Specify the regular expression.
    - The destination domain regex is the same as the destination domain, but the destination domain regex allows you to use standard expression matching on originating server names.

- **destination-ip [<IP/M>|any]**
  - Optional. Specifies the destination server’s IP address, obtained from the HTTP request URL
    - <IP/M> – Specify the destination server’s IP address and mask. This is used as the match criteria.
    - any – Select to specify any destination IP address as the match criteria.
    - **Note:** Provide the IP address in the A.B.C.D/M format.
    - **Note:** Specify any to consider all servers.

- **mimetype-regex <WORD>**
  - Optional. Specifies the regular expression used to match the mimetype of a HTTP request
### Examples

```
nx4500-5CFA2B(config-smart-cache-policy-test)#http-access precedence 4 deny destination-domain .TechPubs
```

```
nx4500-5CFA2B(config-smart-cache-policy-test)#show context smart-cache-policy test
   forward-proxy vlan 10-20
   cache size 30
   aging precedence 1 ignore-case \.".jgp\$ min-age 100 freshness-factor 75 max-age 200
   reload-into-ims
   http-access precedence 4 deny destination-domain .TechPubs
   access-log rotate 10 rotate-type duration 10 day
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes an ACL</td>
</tr>
</tbody>
</table>
4.1.92.2.6 no

smart-cache-policy-mode commands

Removes or resets smart cache policy settings

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [access-log|aging|cache|forward-proxy|http-access|parent-proxy|pre-fetch|
smart-cache|transparent-proxy]

Parameters

- no <PARAMETERS>

no <PARAMETERS> Removes or reverts this Smart Cache policy’s settings based on the parameters passed

Examples

The following example displays the content cache policy ‘test’ settings before the no commands are executed:

```
nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
  forward-proxy vlan 10-2
  aging precedence 1 ignore-case \\.jgp$ min-age 100 freshness-factor 75 max-age 200 preload-into-ims
  http-access precedence 4 deny destination-domain .TechPubs
  access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

```
nx4500-5CFA2B(config-content-cache-policy-test)#no forward-proxy vlan 10-20
nx4500-5CFA2B(config-smart-cache-policy-test)#no aging precedence 1
nx4500-5CFA2B(config-smart-cache-policy-test)#no access-log rotate
```

The following example displays the content cache policy ‘test’ settings after the no commands are executed:

```
nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
  cache size 30
  http-access precedence 4 deny destination-domain .TechPubs
nx4500-5CFA2B(config-smart-cache-policy-test)#
```
4.1.92.2.7 pre-fetch

smart-cache-policy-mode commands

Pre-fetches a specified list of URLs (whose credentials can be stored in the local cache)
This command allows the content cache engine to pre-fetch URLs specified in a URL list. The pre-fetch function is performed immediately or at a scheduled time, based on configuration.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
pre-fetch <URL-LIST-NAME> schedule <TIME>

Parameters
- pre-fetch <URL-LIST-NAME> schedule <TIME>

<URL-LIST-NAME> | Pre-fetches a list of URLs identified by the <URL-LIST-NAME> keyword. URL lists are used to select highly utilized URLs for smart caching. The selected URLs are monitored and routed according to existing cache content policies. The URL list should be existing and configured. For more information on configuring URL lists, see url-list.

schedule <TIME> | Pre-fetches the specified URL list at a specified time.
- <TIME> – Specify the time in the HH:MM format.

Examples
nx4500-5CFA2B(config-content-cache-policy-test)#pre-fetch test schedule 12:30
nx4500-5CFA2B(config-content-cache-policy-test)#show context content-cache-policy test
forward-proxy vlan 10-20
cache media all
cache size 30
http-access precedence 100 deny destination-domain test destination-domainregex test
access-log rotate 10 every 50 day
pre-fetch test schedule 12:30
nx4500-5CFA2B(config-content-cache-policy-test)#

Related Commands
- no Removes an ACL
4.1.92.2.8 parent-proxy

smart-cache-policy-mode commands

Enables upper-layer parent proxy on this smart cache policy

The parent proxy server requires users to authenticate to access Web sites like WinRoute. This setting is disabled by default.

Supported in the following platforms:

• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

parent-proxy [enable|host <IP/HOST-NAME> port <1-32768>]

Parameters

- parent-proxy [enable|host <IP/HOST-NAME> port <1-32768>]

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables parent proxy on this smart cache policy</th>
</tr>
</thead>
</table>
| host <IP/HOST-NAME> port <1-32768> | Configures the hostname or IP address of the parent proxy server

- <IP/HOST-NAME> – Specify the parent proxy server's IP address or hostname.
- port <1-32768> – Specify the TCP port number for the parent proxy server. The default port is 8080.

Examples

nx4500-5CFA2B(config-smart-cache-policy-test)#parent-proxy host 192.168.13.8 port 21

nx4500-5CFA2B(config-smart-cache-policy-test)#show context

parent-proxy host 192.168.13.8 port 21

http-access precedence 4 deny destination-domain .TechPubs

Related Commands

| no | Disables parent proxy on this smart cache policy |
4.1.92.2.9 smart-cache

*smart-cache-policy-mode commands*

Enables smart content caching

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
smart-cache enable

**Parameters**
- smart-cache enable

| smart-cache enable | Enables smart content caching. When enabled, devices using this smart-cache policy act as forward proxy. |

**Examples**
nx4500-5CFA2B(config-smart-cache-policy-test)#smart-cache enable
nx4500-5CFA2B(config-smart-cache-policy-test)#

**Related Commands**
- no | Disables smart content caching |
4.1.92.2.10 transparent-proxy

*smart-cache-policy-mode commands*

Enables the transparent proxy mode on a device. This is the default mode of proxying.
When enabled, all packets are automatically routed to the port on which the content cache engine listens (3128) by default. The advantage of the transparent proxy mode is that clients need not be configured with an explicit proxy.

Transparent content caching, on the other hand, acts as an intermediary for the originating servers and returns cached content to clients as if the data originated from the associated servers. Transparent caching proxies perform server load-balancing and compression to regulate load on the originating servers and reduce bandwidth usage.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
transparent-proxy {protocol|vlan}
transparent-proxy {protocol {all|https}}
transparent-proxy {vlan <VLAN-ID>}
```

**Parameters**

- `transparent-proxy {protocol {all|https}}`
  - Optional. Selects the protocols used for transparent proxy mode
    - `https` – Optional. Enables HTTPS for transparent proxy
    - `all` – Optional. Enables all protocols for transparent proxy
  - `transparent-proxy {vlan <VLAN-ID>}`
    - Optional. Configures the VLAN(s) for which transparent proxy mode (content caching) is enabled. By default content caching is disabled on all VLANs.
    - `<VLAN-ID>` – Specify the list of VLANs.

**Examples**

```
nx4500-5CFA2B(config-smart-cache-policy-test)#transparent-proxy vlan 10-20

nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
  parent-proxy host 192.168.13.8 port 21
  transparent-proxy vlan 10-20
  cache size 30
  http-access precedence 4 deny destination-domain .TechPubs
```

**Related Commands**

- `no`Resets or removes transparent caching proxy settings
4.1.93 url-filter

The following table lists the commands that allow you to enter the URL filter configuration mode:

Table 4.43 Commands Creating a URL Filter

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>url-filter</td>
<td>Creates a new URL filter and enters its configuration mode</td>
<td>page 4-468</td>
</tr>
<tr>
<td>url-filter-config-mode commands</td>
<td>Summarizes the URL filter configuration mode commands</td>
<td>page 4-471</td>
</tr>
</tbody>
</table>
4.1.93.1 url-filter

Creating a new URL filter (Web filter) and enters its configuration mode. URL filtering is a licensed feature. When applied to a WiNG device the license allows you to enable URL filtering on the device, create and apply a URL filter defining the banned and/or allowed URLs. When enabled, the URL filter is applied to all user-initiated URL requests to determine if the requested URL is banned or allowed. Only if allowed is the user’s request (in the form of a HTTP request packet) forwarded to the Web server.

URL filters can be applied at any of the following points: the user’s application (browser/email reader), the network’s gateway, at the Internet service provider’s (ISP) end, and also on a Web portal. For wireless clients, the WLAN infrastructure is the best place to implement these filters.

A URL filter is a set of whitelist and/or blacklist rules. The whitelist allows access only to those Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the whitelist, are banned. On the other hand, the blacklist bans all Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the blacklist, are allowed.

To simplify URL filter configuration, Websites have been classified into pre-defined category-types and categories. The system provides 12 category-types and 64 categories. To further simplify configuration, these 12 category-types have been grouped into five (5) pre-defined levels. (See Usage Guidelines section for the list of category-types, categories, and levels). The actual classification of URLs (on the basis of the pre-defined factors mentioned above) is done by the classification server. A local database also helps by caching URL records for a user-defined time period. The classification server host is specified in the Web filter policy. The Web filter policy also defines the URL database parameters. For more information, see web-filter-policy.

The WiNG software also allows you to create URL lists. Each URL list contains a list of user-defined URLs. Use the URL list in a URL filter (whitelist or blacklist rule) to identify the URLs to ban or allow. For example, a URL list named SocialNetworking is created listing the following three sites: Facebook, Twitter, and LinkedIn. When applied to a URL filter’s blacklist these three sites are banned. Where as, when applied to a whitelist only these three sites are allowed. For more information on configuring a URL list, see url-list.

---

**NOTE:** URL filtering is a licensed feature. Procure and install the license in the device configuration mode. For more information, see license.

---

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

`url-filter <URL-FILTER-NAME>`

**Parameters**

- `url-filter <URL-FILTER-NAME>`

| `<URL-FILTER-NAME>` | Creates a new URL filter and enters its configuration mode. Specify the URL filter name. If the filter does not exist, it is created. |
## Usage Guidelines

<table>
<thead>
<tr>
<th>Category Type</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Adult Content</td>
<td>Alcohol &amp; Tobacco, Dating &amp; Personals, Gambling, Nudity, Pornography/Sexually Explicit, Sex Education, Weapons</td>
</tr>
<tr>
<td>2 Business</td>
<td>Web-based Email</td>
</tr>
<tr>
<td>3 Communication</td>
<td>Chat, Instant Messaging</td>
</tr>
<tr>
<td>4 Entertainment</td>
<td>Streaming Media &amp; Downloads</td>
</tr>
<tr>
<td>5 File Sharing and Backup</td>
<td>Download Sites</td>
</tr>
<tr>
<td>6 Gaming</td>
<td>Games</td>
</tr>
<tr>
<td>8 Peer-to-Peer (P2P)</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>9 Questionable/Unethical</td>
<td>Child Abuse Images, Cults, Hacking, Hate &amp; Intolerance, Illegal Drug, Illegal Sharing, Illegal Software, School Cheating, Tasteless, Violence</td>
</tr>
<tr>
<td>10 Security Risk</td>
<td>Advertisement &amp; Pop-ups, Anonymizers, Botnets, Compromised, Criminal Activity, Malware, Parked Domains, Phishing &amp; Fraud, Spam Sites</td>
</tr>
<tr>
<td>11 Social and Photo Sharing</td>
<td>Social Networking</td>
</tr>
<tr>
<td>12 Software Update</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Basic</td>
<td>Blocks sites/URL categorized as Security Risk</td>
</tr>
<tr>
<td>2 Low</td>
<td>Blocks sites/URL categorized as Adult Content + Basic</td>
</tr>
<tr>
<td>3 Medium</td>
<td>Blocks sites/URL categorized as File Sharing and Backup, P2P, Questionable / Unethical + Low</td>
</tr>
<tr>
<td>4 Medium High</td>
<td>Blocks sites/URL categorized as Gaming + Medium</td>
</tr>
<tr>
<td>5 High</td>
<td>Blocks sites/URL categorized as Communication, Entertainment, Social and Photo Sharing + Medium High</td>
</tr>
</tbody>
</table>
Examples

nx4500-5CFA2B(config-url-filter-test)#?

URL Filter Mode commands:

  blacklist  Block access to URL
  blockpage  Configure blocking page parameters
  description Url filter description
  no         Negate a command or set its defaults
  whitelist  Allow access to URL

  clrscr     Clears the display screen
  commit     Commit all changes made in this session
  do         Run commands from Exec mode
  end        End current mode and change to EXEC mode
  exit       End current mode and down to previous mode
  help       Description of the interactive help system
  revert     Revert changes
  service    Service Commands
  show       Show running system information
  write      Write running configuration to memory or terminal

nx4500-5CFA2B(config-url-filter-test)#
4.1.93.2 url-filter-config-mode commands

url-filter

The following table summarizes URL filter configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist</td>
<td>Creates a blacklist rule defining a list of banned Websites and URLs</td>
<td>page 4-472</td>
</tr>
<tr>
<td>blockpage</td>
<td>Configures the parameters that retrieve the page or content displayed by the client’s browser when a requested URL is blocked and cannot be viewed</td>
<td>page 4-474</td>
</tr>
<tr>
<td>description</td>
<td>Configures an appropriate description for this URL filter</td>
<td>page 4-476</td>
</tr>
<tr>
<td>no</td>
<td>Removes this URL filter’s configured parameters</td>
<td>page 4-477</td>
</tr>
<tr>
<td>whitelist</td>
<td>Creates a whitelist rule defining a list of Websites and URLs allowed access by clients.</td>
<td>page 4-478</td>
</tr>
</tbody>
</table>
4.1.93.2.1 blacklist

**url-filter-config-mode commands**

Creates a blacklist rule. A blacklist is a list of Websites and URLs denied access by clients. Clients requesting blacklisted URLs are presented with a page displaying the 'Web page blocked' message. Parameters relating to this page are configured using the 'blockpage' option.

URL filtering is based on the classification of Websites into pre-defined category-types. Some of the category-types are further divided into multiple categories. Currently available are 12 built-in category types, and 64 categories. These built-in category-types and categories cannot be modified.

Use the available options to identify the URL category-types and categories to include in the blacklist.

In addition to identifying URLs by the categories and category-types they are classified into, the system also provides five (5) levels of Web filtering (basic, high, low, medium, and medium-high). Each level identifies a specific set of URL categories to blacklist. For more information on category-types, categories, and URL filtering levels, see `url-filter`.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

blacklist [category-type|level|url-list]

blacklist category-type [adult-content|all|business|communication|entertainment|file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}

blacklist level [basic|high|low|medium|medium-high] precedence <1-500> {description <LINE>}

blacklist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}

**Parameters**

- blacklist category-type [adult-content|all|business|communication|entertainment|file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}

| blacklist category-type <SELECT-CATEGORY-TYPE> | Selects the category-type to blacklist. A category is a pre-defined URL list available in the WiNG software. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the URL List and added to the database. Websites have been classified into the following 12 category types: adult-content, business, communication, entertainment, file-sharing-backup, gaming, news-sports-general, p2p, questionable, security-risk, social-photo-sharing, and software-updates. Select ‘all’ to blacklist all category-types. Some of the category-types are further classified into categories. For example, the ‘adult-content’ category-type is differentiated into the following categories: alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons. The system blocks all categories (URLs falling within their limits) within the selected category-type. |
| precedence <1-500> | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first. |
### Description <LINE>
Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule.

### blacklist level [basic|high|low|medium|medium-high] precedence <1-500> {description <LINE>}
- **blacklist level**
  - Configures the Web filtering level as basic, high, low, medium, or medium-high. Each of these filter-levels are pre-configured to use a set of category types and this mapping cannot be modified.

### precedence <1-500>
- Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.

### description <LINE>
Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule.

### blacklist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}
- **blacklist url-list**
  - Associates a URL list with this URL filter. When associated with a blacklist rule, all URLs listed in the specified URL list are blacklisted.
  - URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories.
  - For more information on configuring a URL list, see [url-list](#).
  - **<URL-LIST-NAME>** – Enter URL list name (should be existing and configured)

### precedence <1-500>
- Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.

### description <LINE>
Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule.

### Examples
```
rfs7000-6DCD4B(config-url-filter-test)#blacklist level medium-high precedence 10
rfs7000-6DCD4B(config-url-filter-test)#blacklist category-type adult-content category alcohol-tobacco precedence 1
rfs7000-6DCD4B(config-url-filter-test)#blacklist category-type security-risk category botnets precedence 3
rfs7000-6DCD4B(config-url-filter-test)#show context
url-filter test
blacklist level medium-high precedence 10
blacklist category-type security-risk category botnets precedence 3
blacklist category-type adult-content category alcohol-tobacco precedence 1
rfs7000-6DCD4B(config-url-filter-test)#
```

### Related Commands
```
no
```
- Removes a blacklist rule from this URL filter. Specify the category-type, category, and precedence to identify the blacklist rule. The identified rule is removed from the URL filter.
## 4.1.93.2.2 blockpage

### url-filter-config-mode commands

Configures the parameters that retrieve the page or content displayed by the client’s browser when a requested URL is blocked and cannot be viewed.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`blockpage [external</td>
<td>internal</td>
</tr>
<tr>
<td>`blockpage path [external</td>
<td>internal]`</td>
</tr>
<tr>
<td><code>blockpage external url &lt;URL&gt;</code></td>
<td>Configures the internally hosted blocking page parameters, such as the content displayed, page footer and header, organization (the organization enforcing the Web page blocking) details (name, signature, and logo), and page title.</td>
</tr>
<tr>
<td>`blockpage internal [content</td>
<td>footer</td>
</tr>
</tbody>
</table>

### Parameters

- **blockpage path [external|internal]**

  Specifies if the location of the page displayed, to the client when a requested URL is blocked, is external or internal.
  - **external** – Indicates the page displayed is hosted on an external Web server resource. If selecting this option, use the `blockpage > external > url <URL>` command to provide the path to the external Web server hosting the page.
  - **internal** – Indicates the page displayed is hosted internally. This is the default setting. If selecting this option, use the `blockpage > internal > <SELECT-PAGE-TYPE> > <LINE/IMAGE-URL>` command to define the page configuration.

- **blockpage external url <URL>**

  Configures the URL of the external Web server hosting the page (displayed to the client when a requested URL is blocked).
  - **url <URL>** – Specify the URL of the Web server and the blocking page name.
    Valid URLs should begin with `http://` or `https://`.
    The URL can contain query strings.
    Use ‘&’ or ‘?’ character to separate field-value pair.
    Enter `ctrl-v` followed by ‘?’ to configure query strings.

- **blockpage internal [content|footer|header|main-logo|org-name|org-signature|small-logo|title] <LINE/IMAGE-URL>**

  Configures the internally hosted blocking page parameters, such as the content displayed, page footer and header, organization (the organization enforcing the Web page blocking) details (name, signature, and logo), and page title.
  - **content** – Configures the text (message) displayed on the blocking page.
Examples

rfs7000-6DCD4B(config-url-filter-test)#blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
rfs7000-6DCD4B(config-url-filter-test)#show context url-filter test blacklist level medium-high precedence 10 blacklist category-type security-risk category botnets precedence 3 blacklist category-type adult-content category alcohol-tobacco precedence 1 blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
rfs7000-6DCD4B(config-url-filter-test)#

Related Commands

no Removes the blocking page configurations
4.1.93.2.3 description

- url-filter-config-mode commands

Configures a description for this URL filter. Provide a description that enables you to identify the purpose of this URL filter.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax
description <LINE>

Parameters
- description <LINE>

| description <LINE> | Enter an appropriate description for this URL filter. The description should identify the URL filter’s purpose and should not exceed 80 characters in length. |

Examples
rfs7000-6DCD4B(config-url-filter-test)#description "Blacklists sites inappropriate for children and are security risks"
rfs7000-6DCD4B(config-url-filter-test)#show context url-filter test
description "Blacklists\ sites\ inappropriate\ for\ children\ and\ are\ security\ risks"
blacklist level medium-high precedence 10
blacklist category-type security-risk category botnets precedence 3
blacklist category-type adult-content category alcohol-tobacco precedence 1
blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
rfs7000-6DCD4B(config-url-filter-test)#

Related Commands
- no Removes this URL filter’s description
4.1.93.2.4 no

► url-filter-config-mode commands

Use the no command to remove this URL filter’s configured parameters

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax
no [blacklist|blockpage|description|whitelist]
no blacklist [category-type|level|url-list]
no blacklist [category-type <SELECT-CATEGORY-TYPE>|level <SELECT-LEVEL>|url-list <URL-LIST-NAME>] precedence <1-500>
no blockpage [external|internal [content|footer|header|main-logo|org-name|org-signature|small-logo|title]|path]
no description
no whitelist [category-type|url-list]
no whitelist [category-type <SELECT-CATEGORY-TYPE>|url-list <URL-LIST-NAME>] precedence <1-500>

Parameters
- no <PARAMETERS>

no <PARAMETERS> Removes this URL filter’s configured parameters based on the values passed here

Examples
The following example displays the URL filter ‘test’ settings before the ‘no’ is executed:

rfs7000-6DCD4B(config-url-filter-test)#show context
url-filter test
description "Blacklists sites inappropriate for children and are security risks"
blacklist level medium-high precedence 10
blacklist category-type communication category chat precedence 7
blacklist category-type security-risk category botnets precedence 3
blacklist category-type adult-content category alcohol-tobacco precedence 1
blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
rfs7000-6DCD4B(config-url-filter-test)#

rfs7000-6DCD4B(config-url-filter-test)#no description
rfs7000-6DCD4B(config-url-filter-test)#no blacklist category-type adult-content category alcohol-tobacco precedence 1
rfs7000-6DCD4B(config-url-filter-test)#no whitelist category-type communication category chat precedence 7

The following example displays the URL filter ‘test’ settings after the ‘no’ is executed:

rfs7000-6DCD4B(config-url-filter-test)#show context
url-filter test
blacklist level medium-high precedence 10
blacklist category-type security-risk category botnets precedence 3
blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
rfs7000-6DCD4B(config-url-filter-test)#
4.1.93.2.5 whitelist

url-filter-config-mode commands

Creates a whitelist rule. A whitelist is a list of Websites and URLs allowed access by clients.

URL filtering is based on the classification of Websites into pre-defined category-types. Some of the category-types are further divided into multiple categories. Currently available are 12 built-in category types, and 64 categories. These built-in category-types and categories cannot be modified.

Use the available options to identify the category-types and categories to include in the whitelist.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

whitelist [category-type|url-list]
whitelist category-type [adult-content|all|business|communication|entertainment|file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}
whitelist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}

Parameters

- category-type [adult-content|all|business|communication|entertainment|file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}

selects the category-type to add to this whitelist. A category is a pre-defined URL list available in the WiNG software. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the URL List and added to the database.

Websites have been classified into the following 12 category types: adult-content, business, communication, entertainment, file-sharing-backup, gaming, news-sports-general, p2p, questionable, security-risk, social-photo-sharing, and software-updates.

Select 'all' to whitelist all category-types.

Some of the category-types are further classified into categories. For example, the 'adult-content' category-type is differentiated into the following categories:

- alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons.

The system allows all categories (URLs falling within their limits) within the selected category-type.

precedence <1-500> Configures the precedence value for this whitelist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.

description <LINE> Optional. Configures a description (not exceeding 80 characters) for this whitelist rule. Enter a description that allows you to identify the purpose of the rule.
**whitelist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>**

<table>
<thead>
<tr>
<th>whitelist url-list &lt;URL-LIST-NAME&gt;</th>
<th>Associates a URL list with this URL filter. When associated with a whitelist rule, all URLs listed in the specified URL list are allowed access. URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories. For more information on configuring a URL list, see <code>url-list</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>precedence &lt;1-500&gt;</td>
<td>Configures the precedence value for this whitelist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.</td>
</tr>
<tr>
<td>description &lt;LINE&gt;</td>
<td>Optional. Configures a description (not exceeding 80 characters) for this whitelist rule. Enter a description that allows you to identify the purpose of the rule.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-6DCD4B(config-url-filter-test)#whitelist category-type communication category chat precedence 7

rfs7000-6DCD4B(config-url-filter-test)#show context
url-filter test
  description "Blacklists sites inappropriate for children and are security risks"
  blacklist level medium-high precedence 10
  whitelist category-type communication category chat precedence 7
  blacklist category-type security-risk category botnets precedence 3
  blacklist category-type adult-content category alcohol-tobacco precedence 1
  blcokpage internal content "The requested Web page is blocked and cannot be displayed for viewing"

rfs7000-6DCD4B(config-url-filter-test)#
```

**Related Commands**

| no | Removes a whitelist rule from this URL filter. Specify the category-type, category, and precedence to identify the blacklist rule. The identified rule is removed from the URL filter. |
4.1.94 url-list

*Global Configuration Commands*

The following table lists the commands that allow you to enter the URL list configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>url-list</td>
<td>Creates a new URL list and enters its configuration mode</td>
<td>page 4-481</td>
</tr>
<tr>
<td>url-list-config-mode</td>
<td>Summarizes the URL list configuration mode commands</td>
<td>page 4-482</td>
</tr>
</tbody>
</table>
4.1.94.1 url-list

url-list

Creates a URL list and enters its configuration mode. After creating the URL list, add URL entries to the list.

URL lists are used to pre-fetch content from the listed URLs. URL Lists are used to select highly utilized URLs for smart caching. The selected URLs are monitored and routed according to existing cache content policies. To enable pre-fetching of cached content, use the `smart-cache > pre-fetch-immediate > <URL-LIST-NAME>` command. For more information, see `smart-cache`.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
url-list <URL-LIST-NAME>
```

Parameters

- `url-list <URL-LIST-NAME>`

Examples

```
nx4500-5CFA2B(config)#url-list URLlist1
```

```
nx4500-5CFA2B(config-url-list-URLlist1)#?
```

```
URL List Mode commands:
  description  Description of the category
  no           Negate a command or set its defaults
  url          Add a URL entry
  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal
```

```
nx4500-5CFA2B(config-url-list-URLlist1)#
nx4500-5CFA2B(config-url-list-URLlist1)#url http://www.example_company.com depth 10
```

```
nx4500-5CFA2B(config-url-list-test)#show context
```

```
url-list test
  url http://www.example_company.com depth 10
nx4500-5CFA2B(config-url-list-URLlist1)#
```
4.1.94.2 url-list-config-mode commands

The following table summarizes URL list configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Creates a blacklist rule defining a list of banned Web sites and URLs</td>
<td>page 4-483</td>
</tr>
<tr>
<td>url</td>
<td>Adds URL entries to this URL list</td>
<td>page 4-484</td>
</tr>
<tr>
<td>no</td>
<td>Removes this URL list's settings</td>
<td>page 4-485</td>
</tr>
</tbody>
</table>
4.1.94.2.1 description

Configures a description for this URL list. The description should be unique and enable you to identify the type of URLs listed in the URL list.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

description <LINE>

Parameters

- description <LINE>

Examples

nx4500-5CFA2B(config-url-list-test)#description “This URL list contains social media URLs”
nx4500-5CFA2B(config-url-list-test)#show context
url-list test
description “This URL list contains social media URLs”
nx4500-5CFA2B(config-url-list-test)#

Related Commands

| no | Removes this URL list’s description |
4.1.94.2.2  url

```markdown
url-list-config-mode commands
```

Adds URL entries to this URL list

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
url <WORD> {depth <1-10>}
```

**Parameters**

- `url <WORD> {depth <1-10>}`

<table>
<thead>
<tr>
<th><code>url &lt;WORD&gt; {depth &lt;1-10&gt;}</code></th>
<th>Adds a URL entry</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;WORD&gt;</code> – Specify the URL to add.</td>
<td></td>
</tr>
<tr>
<td><code>depth</code> – Optional. Sets number of levels to be cached. Since Web sites have different parameters to uniquely identify specific content, the same content may be stored on multiple origin servers. Smart caching uses subsets of these parameters to recognize that the content is the same and serves it from cache.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;1-10&gt;</code> – Specify the depth from 1 - 10.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
nx4500-5CFA2B(config-url-list-test)#url http://www.facebook.com
```

```
nx4500-5CFA2B(config-url-list-test)#show context
description "This URL list contains social communication URLS"
url https://www.facebook.com depth 5
```

```
nx4500-5CFA2B(config-url-list-test)#
```

**Related Commands**

```
no
```

Removes a URL entry from this URL list
4.1.94.2.3 no

**url-list-config-mode commands**

Removes this URL list's settings

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

no [description|url]

no description

no url <WORD>

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Removes this URL's settings based on the parameters passed |

**Examples**

The following example displays the URL list 'test' settings before the 'no' command is executed:

```shell
nx4500-5CFA2B(config-url-list-test)#show context
url-list test
description "This URL list contains social communication URLs"
url https://www.facebook.com depth 5
```

```shell
nx4500-5CFA2B(config-url-list-test)#no url www.facebook.com
```

The following example displays the URL list 'test' settings after the 'no' command is executed:

```shell
nx4500-5CFA2B(config-url-list-test)#show context
url-list test
description "This URL list contains social communication URLs"
```
4.1.95 vx9000

Global Configuration Commands

Configures a Virtual WLAN Controller (V-WLC) in a virtual machine (VM) environment. V-WLC can be deployed on a shared, third-party server hardware, thereby reducing overhead costs of procuring and maintaining dedicated appliances. The external, third-party hardware needs to have installed hypervisors, such as VmWare, Xen, VirtualBox, KVM, Amazon EC2 or Hyper-V, enabling it to communicate with V-WLC software.

The V-WLC controls and manages access points and other controllers (at NOC or as a site-controller) in the network. The traffic between the access points and the V-WLC is over the layer-3 MINT protocol.

V-WLC is a licensed feature, and the WiNG software provides the following two new licenses:

- **VX** – When installed, this license activates VM controller instance, and enables the V-WLC to trigger adoption process allowing access points to adopt to the V-WLC. The adoption capacity of the V-WLC is determined by the number of licenses installed on it.

- **VX-DEMO** – This is a 60 day trial license. This license also activates VM controller instance, and enables the V-WLC to adopt access points. But, the access point adoption capacity is limited to 16. Having installed this license on a device, the only other license that you can install on it is the VX license. All existing installed licenses will continue to work as before. Since this license has a limited validity period, ensure that the system clock on the license generating tool and the device are in sync. preferably through NTP.

To install the VX or VX-DEMO license on an existing V-WLC instance, use the license command. For more information, see the examples provided in this section.

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

\[ vx9000 \ <\text{MAC}> \]

**Parameters**

- **vx9000** \ <MAC>

**vx <MAC>**

<table>
<thead>
<tr>
<th>vx &lt;MAC&gt;</th>
<th>Configures a V-WLC and enters its configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> The V-WLC configuration is the same as that of a normal controller.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

nx9500-6C8809(config)#vx9000 11-22-33-44-55-66
nx9500-6C8809(config-device-11-22-33-44-55-66)#?

Device Mode commands:

- adopter-auto-provisioning-policy-lookup
- adoption
- adoption-site
- alias
- application-policy
- area
- arp
- auto-learn-staging-config
- autogen-uniqueid
- autoinstall
- bridge
- captive-portal
- cdp
- channel-list
- cluster
- configuration-persistence

Use centralized auto-provisioning policy when adopted by another controller
Adoption configuration
Set system's adoption site
Alias
Application Policy configuration
Set name of area where the system is located
Address Resolution Protocol (ARP)
Enable learning network configuration of the devices that come for adoption
Autogenerate a unique id
Autoinstall settings
Ethernet bridge
Captive portal
Cisco Discovery Protocol
Configure channel list to be advertised to wireless clients
Cluster configuration
Enable persistence of configuration
GLOBAL CONFIGURATION COMMANDS

**contact** Configure the contact
**controller** WLAN controller configuration
**country-code** Configure the country of operation
**critical-resource** Critical Resource
**crypto** Encryption related commands
**database-backup** Scheduled Database Backup
**device-upgrade** Device firmware upgrade
**dot1x** 802.1X Enable Deep-Packet-Inspection (Application Assurance)
**dpi** Configure IP DSCP to 802.1p priority mapping for untagged frames
**dscp-mapping** Configure layout coordinates for this device
**email-notification** Email notification configuration
**enforce-version** Check the firmware versions of devices before interoperating
**environmental-sensor** Environmental Sensors Configuration
**events** System event messages
**export** Export a file
**file-sync** File sync between controller and adoptees
**floor** Set the floor within an area where the system is located
**geo-coordinates** Configure geo coordinates for this device
**gre** GRE protocol
**hostname** Set system's network name
**http-analyze** Specify HTTP-Analysis configuration
**interface** Select an interface to configure
**ip** Internet Protocol (IP)
**ipv6** Internet Protocol version 6 (IPv6)
**l2tpv3** L2tpv3 protocol
**l3e-lite-table** L3e lite Table
**layout-coordinates** Configure layout coordinates for this device
**led** Turn LEDs on/off on the device
**led-timeout** Configure the time for the led to turn off after the last radio state change
**legacy-auto-downgrade** Enable device firmware to auto downgrade when other legacy devices are detected
**legacy-auto-update** Auto upgrade of legacy devices
**license** License management command
**lldp** Link Layer Discovery Protocol
**load-balancing** Configure load balancing parameter
**location** Configure the location
**logging** Modify message logging facilities
**mac-address-table** MAC Address Table
**mac-auth** 802.1x Configure MAC address to name mappings
**mac-name** Memory profile to be used on the device
**memory-profile** Configure meshpoint device parameters
**meshpoint-device** Configure meshpoint monitoring interval
**meshpoint-monitor-interval** Check controller connectivity after configuration is received
**min-misconfiguration-recovery-time** MiNT protocol
**mint** Mirroring
**mirror** Check controller connectivity after configuration is received
**misconfiguration-recovery-time** Configure neighbor inactivity timeout
**neighbor-inactivity-timeout** Configure neighbor information exchange interval
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>noc</td>
<td>Configure the noc related setting</td>
</tr>
<tr>
<td>ntp</td>
<td>Ntp server WORD</td>
</tr>
<tr>
<td>offline-duration</td>
<td>Set duration for which a device remains unadopted before it generates offline event</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configure RF Domain level overrides for wlan</td>
</tr>
<tr>
<td>power-config</td>
<td>Configure power mode</td>
</tr>
<tr>
<td>preferred-controller-group</td>
<td>Controller group this system will prefer for adoption</td>
</tr>
<tr>
<td>preferred-tunnel-controller</td>
<td>Tunnel Controller Name this system will prefer for tunneling extended vlan traffic</td>
</tr>
<tr>
<td>radius</td>
<td>Configure device-level radius authentication parameters</td>
</tr>
<tr>
<td>raid</td>
<td>RAID</td>
</tr>
<tr>
<td>reevaluate-everytime</td>
<td>Set the flag to reevaluate autoprovisioning policy everytime</td>
</tr>
<tr>
<td>remove-override</td>
<td>Remove configuration item override from the device (so profile value takes effect)</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>RF Domain Manager</td>
</tr>
<tr>
<td>router</td>
<td>Dynamic routing</td>
</tr>
<tr>
<td>rsa-key</td>
<td>Assign a RSA key to a service</td>
</tr>
<tr>
<td>sensor-server</td>
<td>AirDefense sensor server configuration</td>
</tr>
<tr>
<td>slot</td>
<td>PCI expansion Slot</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Spanning tree</td>
</tr>
<tr>
<td>timezone</td>
<td>Configure the timezone</td>
</tr>
<tr>
<td>traffic-class-mapping</td>
<td>Configure IPV6 traffic class to 802.1p priority mapping for untagged frames</td>
</tr>
<tr>
<td>trustpoint</td>
<td>Assign a trustpoint to a service</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Tunnel Controller group this controller belongs to</td>
</tr>
<tr>
<td>use</td>
<td>Set setting to use</td>
</tr>
<tr>
<td>vrrp</td>
<td>VRRP configuration</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>Publish interface via OSPF/BGP only if the interface VRRP state is not BACKUP</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enable support for 802.11 WEP shared key authentication</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

nx9500-6C8809(config-device-11-22-33-44-55-66)#
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#license ?
  WORD  Feature name (AP/AAP/ADSEC/HTANLT/SMART-CACHE/VX) for which license is to be added

vx-0099CC(config-device-00-0C-29-00-99-CC)~*#license vx 80ee9649eddc94b48b5a35d7eaf8e73b376a51649291714d04c84769b0fc4b3766816878d2739c24
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#com wr
Jan 16 13:48:11 2014: vx-0099CC : %SYSTEM-6-CONFIG_COMMIT: Configuration commit by user 'root' (mapsh) from 'Console'
Jan 16 13:48:11 2014: vx-0099CC : %SYSTEM-6-CONFIG_REVISION: Configuration revision updated to 9 from 8
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#Jan 16 13:48:12 2014: vx-0099CC : %SYSTEM-6-CONFIG_REVISION: Configuration revision updated to 10 from 9
vx-0099CC(config-device-00-0C-29-00-99-CC)~*#vx-0099CC(config-device-00-0C-29-00-99-CC)~*#vx-0099CC(config-device-00-0C-29-00-99-CC)~*#sh licenses
Serial Number : 000C290099CCC0A80001
WARNING: Recommended minimum system resource requirements not met for the current license pack or cluster configs. Please check user guide and reconfigure the system

Device Licenses:
  AP-LICENSE
    String : 
    Value : 10240
  AAP-LICENSE
    String : 
    Value : 10240
  ADVANCED-SECURITY
    String : DEFAULT-ADV-SEC-LICENSE
  VX-LICENSE
    String :
      80ee9649eddc94b48b5a35d7eaf8e73b376a51649291714d04c84769b0fc4b3766816878d2739c24

Cluster Licenses:
  AP-LICENSE
    Value : 10240
    Used : 0
  AAP-LICENSE
    Value : 10240
    Used : 0

Cluster MAX AP Capacity:
  Value : 10240
  Used : 0

Active Members:

<table>
<thead>
<tr>
<th>MEMBER</th>
<th>SERIAL</th>
<th>LIC TYPE</th>
<th>VALUE</th>
<th>BORROWED</th>
<th>TOTAL</th>
<th>NO.APS</th>
<th>NO.AAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-0C-29-00-99-CC 000C290099CCC0A80001 AP</td>
<td>10240</td>
<td>0</td>
<td>10240</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00-0C-29-00-99-CC 000C290099CCC0A80001 AAP</td>
<td>10240</td>
<td>0</td>
<td>10240</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

vx-0099CC(config-device-00-0C-29-00-99-CC)~*#

Related Commands

no | Removes a VX9000 wireless controller
This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. The PRIV EXEC command set contains commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either the USER EXEC or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.
5.1 Common Commands

The following table summarizes commands common to the User Exec, Priv Exec, and Global Config modes:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 5-3</td>
</tr>
<tr>
<td>commit</td>
<td>Commits (saves) changes made in the current session</td>
<td>page 5-4</td>
</tr>
<tr>
<td>exit</td>
<td>Ends and exits the current mode and moves to the PRIV EXEC mode</td>
<td>page 5-5</td>
</tr>
<tr>
<td>help</td>
<td>Displays the interactive help system</td>
<td>page 5-6</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts values to their default settings</td>
<td>page 5-9</td>
</tr>
<tr>
<td>revert</td>
<td>Reverts changes to their last saved configuration</td>
<td>page 5-12</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands to troubleshoot or debug instance configurations</td>
<td>page 5-13</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system information</td>
<td>page 5-50</td>
</tr>
<tr>
<td>write</td>
<td>Writes the system’s running configuration to memory or terminal</td>
<td>page 5-52</td>
</tr>
</tbody>
</table>

**NOTE:** The input parameter <HOSTNAME> cannot include an underscore character. In other words, a device’s hostname cannot contain an underscore.
### 5.1.1 clrscr

**Common Commands**

Clears the screen and refreshes the prompt, irrespective of the mode

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

clrscr

**Parameters**

None

**Examples**

The terminal window or screen before the clrscr command is executed:

```
rfs4000-229D58# device-upgrade ?
  DEVICE-NAME    Name/MAC address of device
     all          Upgrade all devices
    ap621         Upgrade AP621 Device
    ap622         Upgrade AP622 Device
    ap650         Upgrade AP650 Device
    ap6511        Upgrade AP6511 Device
    ap6521        Upgrade AP6521 Device
    ap6522        Upgrade AP6522 Device
    ap6532        Upgrade AP6532 Device
    ap6562        Upgrade AP6562 Device
    ap71xx        Upgrade AP71XX Device
    ap7502        Upgrade AP7502 Device
    ap7522        Upgrade AP7522 Device
    ap7532        Upgrade AP7532 Device
    ap7562        Upgrade AP7562 Device
    ap81xx        Upgrade AP81XX Device
    ap82xx        Upgrade AP82XX Device
  cancel-upgrade Cancel upgrading the device
  load-image     Load the device images to controller for device-upgrades
  rf-domain      Upgrade all devices belonging to an RF Domain
    rfs4000      Upgrade RFS4000 Device
```

rfs4000-229D58#

The terminal window or screen after the clrscr command is executed:

```
rfs4000-229D58#
```
5.1.2 commit

Commits changes made in the active session. Use the commit command to save and invoke settings entered during the current transaction.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

commit {write}{memory}

Parameters

- commit {write}{memory}

<table>
<thead>
<tr>
<th>write</th>
<th>Optional. Commits changes made in the current session</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Optional. Writes to memory. This option ensures current changes persist across reboots.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE#commit write memory
[OK]
rfs7000-37FABE#
5.1.3 exit

Common Commands

The exit command works differently in the User Exec, Priv Exec, and Global Config modes. In the Global Config mode, it ends the current mode and moves to the previous mode, which is Priv Exec mode. The prompt changes from (config)# to #. When used in the Priv Exec and User Exec modes, the exit command ends the current session, and connection to the terminal device is terminated. If the current session has changes that have not been committed, the system prompts you to either do a commit or a revert before terminating the session.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
exit
```

Parameters

None

Examples

```
rfs7000-37FABE(config)#exit
rfs7000-37FABE#
```
5.1.4 help

Common Commands

Describes the interactive help system

Use this command to access the advanced help feature. Use “?” anytime at the command prompt to access the help topic.

Two kinds of help are provided:

• Full help is available when ready to enter a command argument
• Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example ‘show ve?’).

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

help {search}
help {search <WORD>} {detailed|only-show|skip-no|skip-show}

Parameters

• help {search <WORD>} {detailed|only-show|skip-no|skip-show}

<table>
<thead>
<tr>
<th>search &lt;WORD&gt;</th>
<th>Optional. Searches for CLI commands related to a specified target term</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt; – Specify a target term (for example, a feature or a configuration parameter). After specifying the term, select one of the following options: detailed, only-show, skip-no, or skip-show. The system displays information based on the option selected.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>detailed</th>
<th>Optional. Searches and displays help strings in addition to mode and commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>only-show</th>
<th>Optional. Displays only “show” commands. Does not display configuration commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>skip-no</th>
<th>Optional. Displays only configuration commands. Does not display “no” commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>skip-show</th>
<th>Optional. Displays only configuration commands. Does not display “show” commands</th>
</tr>
</thead>
</table>

Examples

rfs7000-37FABE>help search crypto detailed
found more than 64 references, showing the first 64

Context : Command
Command : clear crypto ike sa (A.B.C.D|all)(|on DEVICE-NAME)
\ Clear
\ Encryption Module
\ IKE SA
\ Flush IKE SAs
\ Flush IKE SAs for a given peer
\ Flush all IKE SA
\ On AP/Controller
\ AP/Controller name

: clear crypto ipsec sa(|on DEVICE-NAME)
\ Clear
\ Encryption Module
\ IPSec database
Flush IPSec SAs
On AP/Controller
AP/Controller name
: crypto key export rsa WORD URL (passphrase WORD|) (background|) ...
Encryption related commands

rfs7000-37FABE>help search crypto only-show

Context : Command
Command : show crypto cmp request status(|on DEVICE-NAME)
: show crypto ike sa (version 1|version 2)(peer A.B.C.D|) (detail...
: show crypto ipsec sa (peer A.B.C.D|) (detail|) (on DEVICE-NAME...
: show crypto key rsa (|public-key-detail) (on DEVICE-NAME)
: show crypto pki trustpoints (WORD|all|)(on DEVICE-NAME)

rfs7000-37FABE>help search service skip-show

found more than 64 references, showing the first 64

Context : Command
Command : service block-adopter-config-update
: service clear adoption history(|on DEVICE-NAME)
: service clear captive-portal-page-upload history (|on DEVICE-NAME)
: service clear command-history(|on DEVICE-NAME)
: service clear device-upgrade history (on DEVICE-NAME)
: service clear noc statistics
: service clear reboot-history(|on DEVICE-NAME)
: service clear unsanctioned aps (|on DEVICE-OR-DOMAIN-NAME)
: service clear upgrade-history(|on DEVICE-NAME)
: service clear web-filter cache(|on DEVICE-NAME)
: service clear wireless ap statistics (|AA-BB-CC-DD-EE-FF|)(on...
: service clear wireless client statistics (|AA-BB-CC-DD-EE-FF|)[...]
: service clear wireless controller-mobility-database
: service clear wireless dns-cache(|on DEVICE-OR-DOMAIN-NAME)
: service clear wireless radio statistics (|DEVICE-NAME |(|<1-3>>)...)
: service clear wireless wlan statistics (WLAN) (|on DEVICE-NAME)
: service clear xpath requests (<1-100000>)
: service show block-adopter-config-update
: service show captive-portal servers(|on DEVICE-NAME)
: service show captive-portal user-cache(|on DEVICE-NAME)
: service show cli
: service show client-identity-defaults
: service show command-history(|on DEVICE-NAME)

rfs7000-37FABE>help search mint only-show

Found 25 references for "mint"

Context : Command
Command : show debugging mint (|on DEVICE-OR-DOMAIN-NAME)
: show mint config(|on DEVICE-NAME)
: show mint dis (|details|)(on DEVICE-NAME)
: show mint id(|on DEVICE-NAME)
: show mint info(|on DEVICE-NAME)
: show mint known-adopters(|on DEVICE-NAME)
: show mint links (|details|)(on DEVICE-NAME)
: show mint lsp
: show mint lsp-db (|details AA.BB.CC.DD|)(on DEVICE-NAME)
: show mint m1cp history(|on DEVICE-NAME)
: show mint m1cp(|on DEVICE-NAME)
: show mint neighbors (|details|)(on DEVICE-NAME)
: show mint route(|on DEVICE-NAME)
: show mint stats(|on DEVICE-NAME)
: show mint tunnel-controller (|details|)(on DEVICE-NAME)
: show mint tunneled-vlans (on DEVICE-NAME)
: show wireless mint client (on DEVICE-OR-DOMAIN-NAME)
: show wireless mint client portal-candidates (on DEVICE-NAME (<1-3>))
: show wireless mint client statistics (on DEVICE-OR-DOMAIN-NAME)
: show wireless mint client statistics rf (on DEVICE-OR-DOMAIN-NAME)
: show wireless mint detail (on DEVICE-NAME (<1-3>)) (filter)
: show wireless mint links (on DEVICE-OR-DOMAIN-NAME)
: show wireless mint portal (on DEVICE-OR-DOMAIN-NAME)
: show wireless mint portal statistics (on DEVICE-OR-DOMAIN-NAME)
: show wireless mint portal statistics rf (on DEVICE-OR-DOMAIN-NAME)

rfs7000-37FAE>
5.1.5 no

**Common Commands**

Negates a command or sets its default. Though the `no` command is common to the User Exec, Priv Exec, and Global Config modes, it negates a different set of commands in each mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`no <PARAMETERS>`

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | The no command is common across all configuration modes and sub modes. It resets or reverts settings based on the mode in which executed. For example, when executed in the AAA policy configuration mode, it allows you to reset or revert a specific AAA policy settings. Similarly, when executed in the global configuration mode, it only resets or reverts settings configured in the global configuration mode. |

**Usage Guidelines**

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

**Examples**

Enter configuration commands, one per line. End with CNTL/Z.

```text
rfs7000-37FABE(config)# no ?
aaa-policy                     Delete a aaa policy
aaa-tacacs-policy              Delete a aaa tacacs policy
alias                          Alias
ap621                          Delete an AP621 access point
ap622                          Delete an AP622 access point
ap650                          Delete an AP650 access point
ap6511                         Delete an AP6511 access point
ap6521                         Delete an AP6521 access point
ap6522                         Delete an AP6522 access point
ap6532                         Delete an AP6532 access point
ap6562                         Delete an AP6562 access point
ap71xx                         Delete an AP71XX access point
ap7502                         Delete an AP7502 access point
ap7522                         Delete an AP7522 access point
ap7532                         Delete an AP7532 access point
ap7562                         Delete an AP7562 access point
ap81xx                         Delete an AP81XX access point
ap82xx                         Delete an AP82XX access point
application                   Delete an application
application-policy            Delete an application policy
association-acl-policy        Delete an association-acl policy
auto-provisioning-policy      Delete an auto-provisioning policy
bonjour-gw-discovery-policy   Disable Bonjour Gateway discovery policy
bonjour-gw-forwarding-policy  Disable Bonjour Gateway Forwarding policy
bonjour-gw-query-forwarding-policy Disable Bonjour Gateway Query Forwarding policy
captive-portal                Delete a captive portal
client-identity               Client identity (DHCP Device Fingerprinting)
```
client-identity-group               Client identity group (DHCP Fingerprint
                        Database)
crypto-cmp-policy               CMP policy
customize                        Restore the custom cli commands to
device                           default
device-categorization            Delete device categorization object
dhcp-server-policy               DHCP server policy
dhcpv6-server-policy             DHCPv6 server related configuration
dns-whitelist                    Delete a whitelist object
event-system-policy              Delete a event system policy
ex3500                           EX3500 device
ex3500-management-policy         Delete a ex3500 management policy
ex3500-qos-class-map-policy      Delete a ex3500 qos class-map policy
ex3500-qos-policy-map            Delete a ex3500 qos policy-map
ex3524                           Delete an EX3524 wireless controller
ex3548                           Delete an EX3548 wireless controller
firewall-policy                  Delete firewall policy
global-association-list         Delete a global association list
igmp-snoop-policy                Remove device onboard igmp snoop policy
inline-password-encryption      Disable storing encryption key in the
                                startup configuration file
ip                               Internet Protocol (IP)
ipv6                             Internet Protocol version 6 (IPv6)
ipv6-router-advertisement-policy IPv6 Router Advertisement related
                                 configuration
l2tpv3                           Negate a command or set its defaults
mac                              MAC configuration
management-policy                Delete a management policy
meshpoint                        Delete a meshpoint object
meshpoint-qos-policy             Delete a mesh point QoS configuration
can-list                         Delete an network access control list
nsight-policy                    Delete a nsight policy
passpoint-policy                 Delete a passpoint configuration policy
password-encryption              Disable password encryption in
                                configuration
profile                          Delete a profile and all its associated
                                 configuration
radio-qos-policy                 Delete a radio QoS configuration policy
radius-group                     Local radius server group configuration
radius-server-policy             Remove device onboard radius policy
radius-user-pool-policy          Configure Radius User Pool
rf-domain                        Delete one or more RF-domains and all
                                 their associated configurations
rfs4000                          Delete an RFS4000 wireless controller
rfs6000                          Delete an RFS6000 wireless controller
rfs7000                          Delete an RFS7000 wireless controller
roaming-assist-policy            Delete a roaming-assist policy
role-policy                      Role based firewall policy
routing-policy                   Policy Based Routing Configuration
smart-rf-policy                  Delete a smart-rf-policy
ts                               Delete an TS wireless controller
url-filter                       Delete a url filter
url-list                         Delete a URL list
web-filter-policy                Delete a web filter policy
wips-policy                      Delete a wips policy
wlan                             Delete a wlan object
wlan-qos-policy                  Delete a wireless lan QoS configuration
                                 policy
serve                            Service Commands
rfs7000-37FABE(config)#
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>User Exec Commands mode</td>
</tr>
<tr>
<td>no</td>
<td>Priv Exec Commands mode</td>
</tr>
<tr>
<td>no</td>
<td>Global Config Commands mode</td>
</tr>
</tbody>
</table>
5.1.6 revert

- **Common Commands**
  
  Reverts changes made, in the current session, to their last saved configuration

  Supported in the following platforms:
  
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

revert

**Parameters**

None

**Examples**

rfs7000-37FABE>revert
rfs7000-37FABE>
5.1.7 service

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode. The User Exec mode and Priv Exec mode commands provide same functionalities with a few minor changes. The Global Config service command sets the size of history files. It also enables viewing the current mode's CLI tree.

This section consists of the following sub-sections:

- Syntax (User Exec Mode)
- Syntax (Privilege Exec Mode)
- Syntax (Privilege Exec Mode: NX9000, NX9500, and NX9510)
- Syntax (Global Config Mode)

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax (User Exec Mode)

```
service [block-adopter-config-update|clear|cli-tables-skin|cluster|delete-offline-aps|
force-send-config|force-update-vm-stats|guest-registration|load-balancing|
load-ssh-authorized-keys|locator|radio|radius|request-full-config-from-adopter|
set|show|smart-rf|ssm|snmp|syslog|wireless]
service clear [block-adopter-config-update|request-full-config-from-adopter]
service clear [adoption|captive-portal-page-upload|command-history|device-upgrade|dpi|
file-sync|noc|reboot-history|unsanctioned|upgrade-history|virtual-machine-history|web-filter|wireless|xpath]
service clear adoption history {on <DEVICE-NAME>}
service clear device-upgrade history {on <DOMAIN-NAME>}
service clear dpi [all|app|app-category] stats {on <DEVICE-OR-DOMAIN-NAME>}
service clear file-sync history {on <DOMAIN-NAME>}
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}
service clear [command-history|reboot-history|upgrade-history|virtual-machine-history]
{on <DEVICE-NAME>}
service clear noc statistics
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}
service clear web-filter cache {on <DEVICE-NAME>}
service clear wireless [ap|client|controller-mobility-database|dns-cache|radio|wlan]
service clear wireless controller-mobility-database
service clear wireless [ap|client] statistics {<MAC>} {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless dns-cache on {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless radio statistics {<MAC/hostname>} {<1-3>}
{on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless wlan statistics {<WLAN-NAME>} {on <DEVICE-OR-DOMAIN-NAME>}
service clear xpath requests {<1-100000>}
service cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8]
{grid}
service cluster force [active|configured-state|standby]
service delete-offline-aps [all|offline-for]
service delete-offline-aps offline-for days <0-999> {time <TIME>}
service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}
```
service force-update-vm-stats {on <DEVICE-NAME>}

service guest-registration [backup|delete|export|import]

service guest-registration backup [delete|restore]

service guest-registration delete [all|email <EMAIL-ADD>|mac <MAC>]
  mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>|wlan <WLAN-NAME>

service guest-registration export [csv|json] <DEST-URL> 
  {rfdomain <DOMAIN-NAME> | 
  time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] | wlan <WLAN-NAME>}

service guest-registration import format <JSON> <SOURCE-URL>

service load-balancing clear-client-capability [mac | all] {on <DEVICE-NAME>}

service load-ssh-authorized-keys <PUBLIC-KEY> {on <DEVICE-NAME>}

service locator {<1-60> | {on <DEVICE-NAME>}}

service radio <1-3> [adaptivity|channel-switch|dfs]

service radio <1-3> adaptivity

service radio <1-3> channel-switch <36-196> [160|20|40|80|80-80]

service radio <1-3> dfs simulator-radar [extension|primary]

service radius test [ip|<HOSTNAME>] [word|port]

service radius test [ip|<HOSTNAME>] <word> <USERNAME> <PASSWORD> 
  {wlan <WLAN-NAME> ssid <SSID> | wlan <WLAN-NAME> ssid <SSID>}

service set validation-mode [full|partial] {on <DEVICE-NAME>}

service show [block-adopter-config-update|captive-portal|cli|client-identity-defaults| 
  command-history|configuration-revision|crash-info|dhcp-lease|diag|fast-switching| 
  fib|fib6|guest-registration|info|mac-vendor|mem|mint|noc|pm|process|reboot-history| 
  rf-domain-manager|sites|snmp|ssh-authorized-keys|startup-log|sysinfo|top| 
  upgrade-history|virtual-machine-history|watch-dog|wireless|xpath-history]

service show block-adopter-config-update

service show captive-portal [log-internal|servers|user-cache]

service show captive-portal log-internal

service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}

service show [cli|client-identity-defaults|configuration-revision| 
  mac-vendor <OUI/MAC>|noc diag|snmp session|xpath-history]

service show [command-history|crash-info|info|mem|process|reboot-history|startup-log| 
  ssh-authorized-keys|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}

service show dhcp-lease {INTERFACE-NAME|pppoel|vlan <1-4094>|wwan1}

{on <DEVICE-NAME>}

service show diag [led-status|psu|stats] {on <DEVICE-NAME>}

service show fast-switching {on <DEVICE-NAME>}

service show [fib|fib6] {table-id <0-255>}

service show guest-registration [export-status|import-status|restore-status]

service show mint [adopted-devices {on <DEVICE-NAME>}|ports]

service show pm {history} {on <DEVICE-NAME>}

service show rf-domain-manager [diag|info] {MAC/HOSTNAME}

{on <DEVICE-OR-DOMAIN-NAME>}

{on <DEVICE-NAME>}

service show sites

service show virtual-machine-history {on <DEVICE-NAME>}

service show wireless [aaa-stats|adaptivity-status|client|config-internal| 
  credential-cache|dns-cache|log-internal|meshpoint|neighbors|radar-status| 
  radio-internal|reference|stats-client|vlan-usage]
### COMMON COMMANDS 5-15

```
- `service show wireless [aaa-stats/adaptivity-status|credential-cache|dns-cache|radar-status|vlan-usage] {on <DEVICE-NAME>}`
- `service show wireless [config-internal|log-internal|neighbors]`
- `service show wireless [client|meshpoint neighbor] proc [info|stats] {<MAC>}
  {on <DEVICE-OR-DOMAIN-NAME>}`
- `service show wireless radio-internal [radio1|radio2] <LINE>`
- `service show wireless reference [channels|frame|handshake|mcs-rates|reason-codes|status-codes]`
- `service show wireless stats-client diag {<MAC/HOSTNAME>} {on <DEVICE-OR-DOMAIN-NAME>}`
- `service smart-rf [clear-config|clear-history|clear-interfering-aps|save-config]`
- `service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}`
- `service smart-rf [clear-history]|clear-interfering-aps|save-config {on <DOMAIN-NAME>}`
- `service snmp sysoid wing5`
- `service ssm [dump-core-snapshot|trace]`
- `service ssm trace pattern <WORD> {on <DEVICE-NAME>}`
- `service syslog test {level [0-7]|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings} {on <DEVICE-NAME>}`
- `service wireless [client|dump-core-snapshot|meshpoint|qos|trace|unsanctioned|wips]`
- `service wireless client [beacon-request|quiet-element|trigger-bss-transition|trigger-wnm]`
- `service wireless client beacon-request <MAC> mode [active|passive|table]
  ssid [<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on <DEVICE-NAME>}`
- `service wireless client quiet-element [start|stop]`
- `service wireless client trigger-bss-transition mac <MAC> {timeout <0-65535>} {url <URL>}
  {on <DEVICE-OR-DOMAIN-NAME>}`
- `service wireless client trigger-wnm mac <MAC> type [deauth-imminent|
  subscription-remediation] {uri <WORD>}`
- `service wireless dump-core-snapshot`
- `service wireless meshpoint zl <MESHPOINT-NAME> {on <DEVICE-NAME>}
  {ARGS}|timeout <1-65535>}`
- `service wireless gos delete-tspec <MAC> tid <0-7>`
- `service wireless trace pattern <WORD> {on <DEVICE-NAME>}`
- `service wireless unsanctioned ap air-terminate <MAC> {on <DOMAIN-NAME>}`
- `service wireless wips [clear-client-blacklist|clear-event-history]
  dump-managed-config]`
- `service wireless wips clear-client-blacklist [all]mac <MAC>`
- `service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}`
```

#### Parameters (User Exec Mode)

- **Service**
  - `service [block-adopter-config-update|request-full-config-from-adopter]`

<table>
<thead>
<tr>
<th>block-adopter-config-update</th>
<th>Blocks the configuration updates sent from the NOC server</th>
</tr>
</thead>
<tbody>
<tr>
<td>request-full-config-from-adopter</td>
<td>Configures a request for full configuration updates from the adopter device</td>
</tr>
</tbody>
</table>

In an **hierarchically managed** (HM) network devices are deployed in two levels. The first level consists of the **Network Operations Center** (NOC) controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (access points and site controllers) are referred to as the adoptee. The devices adopting the adoptee are the 'adopters'.
### Service Clear Adoption History

```bash
service clear adoption history {on <DEVICE-NAME>}
```

- **clear adoption history**: Clears adoption history on this device and its adopted access points.
- **on <DEVICE-NAME>**: Optional. Clears adoption history on a specified device.
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

### Service Clear Device Upgrade History

```bash
service clear device-upgrade history {on <DOMAIN-NAME>}
```

- **clear device-upgrade history**: Clears device upgrade history.
- **on <DOMAIN-NAME>**: Optional. Clears all firmware upgrade history in a specified RF Domain.
  - `<DOMAIN-NAME>` – Specify the RF Domain name.

### Service Clear DPI

```bash
service clear dpi [all|app|app-category] stats {on <DEVICE-OR-DOMAIN-NAME>}
```

- **clear dpi**: Clears Deep Packet Inspection (DPI) statistics.
- **[all|app|app-category] stats**: Use the following filter options to clear all or specific DPI statistics:
  - `all` – Clears all DPI related (application and app-category) statistics
  - `app` – Clears only application related statistics
  - `app-category` – Clears only app-category related statistics
- **on <DEVICE-OR-DOMAIN-NAME>**: Optional. Clears DPI statistics based on the parameters passed on a specified device or RF Domain.
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the access point, controller, service platform, or RF Domain.

### Service Clear File Synchronization History

```bash
service clear file-sync history {on <DOMAIN-NAME>}
```

- **clear file-sync history**: Clears client-bridge certificate synchronization statistics.
- **on <DOMAIN-NAME>**: Optional. Clears file synchronization history on all devices within a specified RF Domain.
  - `<DOMAIN-NAME>` – Specify the RF Domain name.

### Service Clear Captive Portal Page Upload History

```bash
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}
```

- **clear captive-portal-page-upload history**: Clears captive portal page upload history.
- **on <DOMAIN-NAME>**: Optional. Clears captive portal page upload history on a specified RF Domain.
  - `<DOMAIN-NAME>` – Specify the RF Domain name.
### COMMON COMMANDS

- **service clear [command-history|reboot-history|upgrade-history|virtual-machine-history] {on <DEVICE-NAME>}

  - **clear [command-history|reboot-history|upgrade-history]**
    - Clears command history, reboot history, or device upgrade history

  - **clear virtual-machine-history**
    - Clears virtual-machine history on the logged device or a specified device
    - **Note:** This command is applicable only on the NX45XX, NX65XX, NX9500, and NX9510 series service platforms.

  - **on <DEVICE-NAME>**
    - Optional. Clears history on a specified device
    - • **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.
    - **Note:** When executing the clear virtual-machine-history command, provide the name of the service platform running the VMs.

- **service clear noc statistics**

  - **clear noc statistics**
    - Clears Network Operations Center (NOC) applicable statistics counters

- **service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}

  - **clear unsanctioned aps**
    - Clears the unsanctioned APs list

  - **on <DEVICE-OR-DOMAIN-NAME>**
    - Optional. Clears the unsanctioned APs list on a specified device or RF Domain
    - • **<DEVICE-OR-DOMAIN-NAME>** – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- **service clear wireless [ap|client] {<MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

  - **clear wireless [ap|client] statistics**
    - Clears wireless statistics counters based on the parameters passed
    - • ap statistics – Clears applicable AP statistics counters
    - • client statistics – Clears applicable wireless client statistics counters
    - • **<DEVICE-OR-DOMAIN-NAME>** – Specify the name of the AP, wireless controller, service platform, or RF Domain.

  - **<MAC>**
    - **on <DEVICE-OR-DOMAIN-NAME>**
      - The following keywords are common to the ‘ap’ and ‘client’ parameters:
      - • **<MAC>** – Optional. Clears statistics counters for a specified AP or client. Specify the AP/client MAC address.
      - • **on <DEVICE-OR-DOMAIN-NAME>** – Optional. Clears AP/client statistics counters on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.

- **service clear wireless controller-mobility-database**

  - **clear wireless controller-mobility-database**
    - Clears the controller assisted mobility database

- **service clear web-filter cache {on <DEVICE-NAME>}

  - **clear web-filter cache**
    - Clears the cache used for Web filtering
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Clears the Web filtering cache on a specified device. <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>• service clear wireless radio statistics <code>{&lt;MAC/HOSTNAME&gt;} {&lt;1-3&gt;} {&lt;on &lt;DEVICE-OR-DOMAIN-NAME&gt;}&gt;</code></td>
<td>Clears applicable wireless radio statistics counters. <code>&lt;MAC/HOSTNAME&gt;</code> <code>&lt;1-3&gt;</code> Optional. Specify the MAC address or hostname of the radio, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE:FF:RX or HOSTNAME:RX format. <code>&lt;1-3&gt;</code> – Optional. Specify the radio interface index, if not specified as part of the radio ID. <code>&lt;on &lt;DEVICE-OR-DOMAIN-NAME&gt;&gt;</code> Optional. This is a recursive parameter, which clears wireless radio statistics on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain. <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code> – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
<tr>
<td>clear wireless wlan statistics</td>
<td>Clears WLAN statistics counters. <code>&lt;WLAN-NAME&gt;</code> Optional. Clears statistics counters on a specified WLAN. Specify the WLAN name. <code>&lt;on &lt;DEVICE-OR-DOMAIN-NAME&gt;&gt;</code> Optional. This is a recursive parameter, which clears WLAN statistics on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain. <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code> – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
<tr>
<td>• service clear xpath requests <code>{&lt;1-100000&gt;}</code></td>
<td>Clears XPATH related information. <code>&lt;1-100000&gt;</code> Optional. Specifies the session number (cookie from show sessions). <code>&lt;1-100000&gt;</code> – Specify the session number from 1 - 100000. Note: Omits clearing the current session’s pending XPATH get requests.</td>
</tr>
</tbody>
</table>
| cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8] {grid} | Selects a formatting layout or skin for CLI tabular outputs. ansi – Uses ANSI characters for borders hashes – Uses hashes (#) for borders minimal – Uses one horizontal line between title and data rows none – Displays space separated items with no decoration percent – Uses the percent sign (%) for borders Contd..
<table>
<thead>
<tr>
<th>COMMON COMMANDS 5-19</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>service cluster force</strong> [active</td>
</tr>
<tr>
<td><strong>cluster</strong> Enables cluster protocol management</td>
</tr>
<tr>
<td><strong>force</strong> Forces action commands on a cluster (active, configured-state, and standby)</td>
</tr>
<tr>
<td><strong>active</strong> Changes the cluster run status to active</td>
</tr>
<tr>
<td><strong>configured-state</strong> Restores a cluster to the configured state</td>
</tr>
<tr>
<td><strong>standby</strong> Changes the cluster run status to standby</td>
</tr>
<tr>
<td><strong>service delete-offline-aps all</strong> Deletes all off-line access points</td>
</tr>
<tr>
<td><strong>delete-offline-aps all</strong> Deletes all off-line access points</td>
</tr>
<tr>
<td><strong>service delete-offline-aps offline-for days &lt;0-999&gt; {time &lt;TIME&gt;}</strong> Deletes off-line access points for a specified interval</td>
</tr>
<tr>
<td><strong>delete-offline-aps</strong> Deletes off-line access points for a specified interval</td>
</tr>
<tr>
<td><strong>day &lt;0-999&gt;</strong> Deletes off-line access points for a specified number of days</td>
</tr>
<tr>
<td><strong>time &lt;TIME&gt;</strong> Optional. Deletes off-line access points for a specified time</td>
</tr>
<tr>
<td><strong>service force-send-config {on &lt;DEVICE-OR-DOMAIN-NAME&gt;</strong> Resends configuration to device(s)</td>
</tr>
<tr>
<td><strong>force-send-config</strong> Resends configuration to device(s)</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</strong> Optional. Resends configuration to a specified device or all devices in a specified RF Domain</td>
</tr>
<tr>
<td><strong>service force-update-vm-stats {on &lt;DEVICE-NAME&gt;</strong> Forcefully pushes VM statistics on to the NOC</td>
</tr>
<tr>
<td><strong>force-update-vm-stats</strong> Forcefully pushes VM statistics on to the NOC</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong> Optional. Executes the command on a specified device</td>
</tr>
<tr>
<td>**service guest-registration backup [delete</td>
</tr>
<tr>
<td>**service guest-registration backup [delete</td>
</tr>
<tr>
<td><strong>delete</strong> – Deletes all guest registration backup snapshots</td>
</tr>
<tr>
<td><strong>restores</strong> – Restores all guest registration backup snapshots</td>
</tr>
<tr>
<td><strong>Note:</strong> To view the status of the restore process, use the <strong>service &gt; show &gt; guest-registration &gt; restore-status</strong> command.</td>
</tr>
</tbody>
</table>
- service guest-registration delete [all|email <EMAIL-ADD>|mac <MAC>|mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>]

    Deletes a specified user or all user records in the database
To delete a specific user, use one of the following options as an identification parameter: email, mac, mobile number, or name

    [all]
    email <EMAIL-ADD>  
    mac <MAC>  
    mobile <MOBILE-NUMBER>  
    name <CLIENT-FULL-NAME>

    Following are the user filtering options: The user identified by one of the following parameters is deleted from the client database.
    • email <EMAIL-ADD> – Identifies user by the e-mail address
    • <EMAIL-ADD> – Provide the user’s e-mail address.
    • mac <MAC> – Identifies user by the MAC address
    • <MAC> – Provide the user’s MAC address.
    • mobile <MOBILE-NUMBER> – Identifies user by the registered mobile number
    • <MOBILE-NUMBER> – Provide the user’s mobile number.
    • name <CLIENT-FULL-NAME> – Identifies user by the registered full name
    • <CLIENT-FULL-NAME> – Provide the user’s full name.

- service guest-registration export format [csv|json] <DEST-URL> { (rfdomain <DOMAIN-NAME>|time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all]|wlan <WLAN-NAME>) }

    Exports guest registration user data files in the Comma-Separated Values (CSV) or JavaScript Object Notation (JSON) format
Use the ‘rfdomain’, ‘wlan’, and ‘time’ options to filter users for a specified RF Domain, WLAN, and/or time period. These are recursive parameters and you can apply all or any of these three filters.

    format [csv|json]  
    <DEST-URL>  
    rfdomain <DOMAIN-NAME>  
    wlan <WLAN-NAME>

    Specifies the file format. The options are:
    • CSV – Exports user data files in the CSV format
    • json – Exports user data files in the JSON format

    Configures the destination URL. The files are exported to the specified location. Both IPv4 and IPv6 address formats are supported.
    IPv4 URLs:
    • tftp://<hostname>[IP][:port]/path/file
    • ftp://<user>:<passwd>@<hostname>[IP][:port]/path/file
    • sftp://<user>:<passwd>@<hostname>[IP][:port]/path/file

    IPv6 URLs:
    • tftp://<hostname>[IPv6][:port]/path/file
    • ftp://<user>:<passwd>@<hostname>[IPv6][:port]/path/file
    • sftp://<user>:<passwd>@<hostname>[IPv6][:port]/path/file

    Optional. Filters user data based on RF Domain name. Only the filtered data are exported.
    • <DOMAIN-NAME> – Specify the RF Domain name.

    Optional. Filters user data based on WLAN name. Only the filtered data are exported.
    • <WLAN-NAME> – Specify the WLAN name.
### COMMON COMMANDS 5-21

<table>
<thead>
<tr>
<th>Time Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Day</td>
<td>Filters and exports previous day’s data</td>
</tr>
<tr>
<td>1-Month</td>
<td>Filters and exports previous month’s data</td>
</tr>
<tr>
<td>1-Week</td>
<td>Filters and exports previous week’s data</td>
</tr>
<tr>
<td>2-Hours</td>
<td>Filters and exports last 2 hours data</td>
</tr>
<tr>
<td>30-Mins</td>
<td>Filters and exports last 30 minutes data</td>
</tr>
<tr>
<td>5-Hours</td>
<td>Filters and exports last 5 hours data</td>
</tr>
<tr>
<td>all</td>
<td>Exports the entire database</td>
</tr>
</tbody>
</table>

- **service guest-registration import format json <SOURCE-URL>**
  - Imports user data from a specified location
  - `format json`: Specifies the file format
    - `json`: Imports user data files in the JSON format
  - `<SOURCE-URL>`: Configures the Source URL. The files are imported from the specified location. Both IPv4 and IPv6 address formats are supported.
    - **IPv4 URLs:**
      - `tftp://<hostname|IP>[:port]/path/file`
      - `ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`
      - `sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`
    - **IPv6 URLs:**
      - `tftp://<hostname|IPv6>[:port]/path/file`
      - `ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file`
      - `sftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file`

- **service load-balancing clear-client-capability [<MAC]|all] {on <DEVICE-NAME>]**
  - Enables wireless load balancing by clearing client capability records
  - `<MAC>`: Clears capability records of a specified client. Specify the client’s MAC address in the AA-BB-CC-DD-EE-FF format.
  - `all`: Clears the capability records of all clients
  - `<DEVICE-NAME>`: Optional. Clears client capability records on a specified device

- **service load-ssh-authorized-keys <PUBLIC-KEY> {on <DEVICE-NAME>]**
  - Loads SSH public (client) key on a device
  - `<PUBLIC-KEY>`: Enter the public key. The public key should be in the OpenSSH rsa/dsa format.
  - `<DEVICE-NAME>`: Optional. Loads the specified public key on a specified device
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| service locator `<1-60>` `(on <DEVICE-NAME>)` | Enables LEDs. Sets LED flashing time from 1 - 60 seconds. The following keyword is recursive and common to the `<1-60>` parameter:  
  - `<on <DEVICE-NAME>>` – Optional. Enables LEDs on a specified device.  
  - `<DEVICE-NAME>` – Specify name of the AP, wireless controller, or service platform. |
| service radio `<1-3>` adaptivity | Configures radio's parameters. `<1-3>` – Specify the radio index from 1 - 3. |
| radio `<1-3>` channel-switch `<36-196>` `[160|20|40|80|80-80]` | Enables channel switching. `<36-196>` – Specifies the channel to switch to from 36 - 196.  
  - `[160|20|40|80|80-80]` – Specifies the bandwidth for the above specified channel. Select the appropriate option. |
| service radius test `<IP>|<HOSTNAME>` `<WORD>` `<USERNAME>` `<PASSWORD>` `{wlan `<WLAN-NAME>` ssid `<SSID>`}` `(on <DEVICE-NAME>)` | Tests RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients.  
  - `<test>` – Tests the RADIUS server's account with user provided parameters.  
  - `<IP>` – Specifies the RADIUS server’s IP address.  
  - `<HOSTNAME>` – Specifies the RADIUS server’s hostname.  
  - `<USERNAME>` – Specify username for authentication.  
  - `<PASSWORD>` – Specify the password. |
### COMMON COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wlan</strong> <code>&lt;WLAN-NAME&gt;</code> <strong>ssid</strong> <code>&lt;SSID&gt;</code></td>
<td>Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.</td>
</tr>
<tr>
<td><strong>on</strong> <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device</td>
</tr>
<tr>
<td><strong>service radius test</strong> <code>&lt;IP&gt;</code> <code>&lt;HOSTNAME&gt;</code></td>
<td>Tests a RADIUS server’s account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients.</td>
</tr>
<tr>
<td><strong>port</strong> <code>&lt;1024-65535&gt;</code></td>
<td>Specify the RADIUS server port. The default port is 1812.</td>
</tr>
<tr>
<td><strong>&lt;WORD&gt;</strong></td>
<td>Specify the RADIUS server’s shared secret.</td>
</tr>
<tr>
<td><strong>&lt;USERNAME&gt;</strong></td>
<td>Specify username for authentication.</td>
</tr>
<tr>
<td><strong>&lt;PASSWORD&gt;</strong></td>
<td>Specify the password.</td>
</tr>
<tr>
<td><strong>wlan</strong> <code>&lt;WLAN-NAME&gt;</code> <strong>ssid</strong> <code>&lt;SSID&gt;</code></td>
<td>Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.</td>
</tr>
<tr>
<td><strong>on</strong> <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device</td>
</tr>
<tr>
<td><strong>service set validation-mode</strong> `[full</td>
<td>partial]`</td>
</tr>
<tr>
<td><strong>set</strong></td>
<td>Sets the validation mode for running configuration validation</td>
</tr>
<tr>
<td><strong>validation-mode</strong> `[full</td>
<td>partial]`</td>
</tr>
<tr>
<td><strong>on</strong> <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Performs full or partial configuration validation on a specified device</td>
</tr>
<tr>
<td><strong>service show block-adopter-config-update</strong></td>
<td>Displays NOC configuration blocking status</td>
</tr>
<tr>
<td><strong>show</strong></td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td><strong>block-adopter-config-update</strong></td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
</tbody>
</table>

**Notes:**
- wlan <WLAN-NAME> ssid <SSID> - Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.
- on <DEVICE-NAME> - Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device.
- service radius test [<IP>|<HOSTNAME>] port 1024-65535 <WORD> <USERNAME> <PASSWORD> wlan <WLAN-NAME> ssid <SSID> on <DEVICE-NAME> - Tests a RADIUS server’s account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients.
- service set validation-mode [full|partial] on <DEVICE-NAME> - Sets the validation mode for running configuration validation.
- service show block-adopter-config-update - Displays NOC configuration blocking status.
- service show captive-portal log-internal - Displays running system statistics based on the parameters passed.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal</td>
<td>Displays captive portal information</td>
</tr>
<tr>
<td>log-internal</td>
<td>Displays recent captive portal debug logs (information and above severity level)</td>
</tr>
</tbody>
</table>

- **service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Displays captive portal information</td>
</tr>
<tr>
<td>servers</td>
<td>Displays server information for active captive portals</td>
</tr>
<tr>
<td>user-cache</td>
<td>Displays cached user details for a captive portal</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays server information or cached user details on a specified device</td>
</tr>
</tbody>
</table>
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- **service show [cli|client-identity-defaults|configuration-revision|mac-user-import-status|mac-vendor <OUI/MAC>|noc diag|snmp session|xpath-history]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>cli</td>
<td>Displays CLI tree of the current mode</td>
</tr>
<tr>
<td>client-identity-defaults</td>
<td>Displays default client-identities and their configuration</td>
</tr>
<tr>
<td>configuration-revision</td>
<td>Displays current configuration revision number</td>
</tr>
<tr>
<td>mac-user-import-status</td>
<td>Displays status of file import initiated by a MAC-user</td>
</tr>
<tr>
<td>mac-vendor &lt;OUI/MAC&gt;</td>
<td>Displays vendor name for a specified MAC address or <em>Organizationally Unique Identifier</em> (OUI) part of the MAC address</td>
</tr>
</tbody>
</table>
  - <OUI/MAC> – Specify the MAC address or its OUI. The first six digits of the MAC address is the OUI. Use the AABBCC or AA-BB-CC format to provide the OUI. |
| noc diag                        | Displays NOC diagnostic details                                             |
| snmp session                    | Displays SNMP session details                                               |
| xpath-history                   | Displays XPath history                                                      |

- **service show [command-history|crash-info|info|mem|process|reboot-history|startup-log|ssh-authorized-keys|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>command-history</td>
<td>Displays command history (lists all commands executed)</td>
</tr>
<tr>
<td>crash-info</td>
<td>Displays information about core, panic, and AP dump files</td>
</tr>
<tr>
<td>info</td>
<td>Displays snapshot of available support information</td>
</tr>
<tr>
<td>mem</td>
<td>Displays a system’s current memory usage (displays the total memory and available memory)</td>
</tr>
<tr>
<td>process</td>
<td>Displays active system process information (displays all processes currently running on the system)</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reboot-history</td>
<td>Displays the device’s reboot history</td>
</tr>
<tr>
<td>startup-log</td>
<td>Displays the device’s startup log</td>
</tr>
<tr>
<td>ssh-authorized-keys</td>
<td>Displays all devices (device hostnames) that have ssh authorized keys loaded</td>
</tr>
<tr>
<td>sysinfo</td>
<td>Displays system’s memory usage information</td>
</tr>
<tr>
<td>top</td>
<td>Displays system resource information</td>
</tr>
<tr>
<td>upgrade-history</td>
<td>Displays the device’s upgrade history (displays details, such as date, time,</td>
</tr>
<tr>
<td>watchdog</td>
<td>Displays the device’s watchdog status</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to all of the above:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays information for a specified device.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service</td>
</tr>
<tr>
<td></td>
<td>platform.</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>dhcp-lease</td>
<td>Displays DHCP lease information received from the server</td>
</tr>
<tr>
<td>&lt;INTERFACE-NAME&gt;</td>
<td>Optional. Displays DHCP lease information for a specified router interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;INTERFACE-NAME&gt; – Specify the router interface name.</td>
</tr>
<tr>
<td>on</td>
<td>Optional. Displays DHCP lease information for a specified device</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Optional. Displays DHCP lease information for a PPP over Ethernet interface</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Optional. Displays DHCP lease information for a VLAN interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify a VLAN index from 1 - 4094.</td>
</tr>
<tr>
<td>wwan1</td>
<td>Optional. Displays DHCP lease information for a Wireless WAN interface</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to all of the above:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays DHCP lease information for a specified device. If no device is specified, the system displays information for the logged device.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>diag</td>
<td>Displays diagnostic statistics, such as LED status, fan speed, and sensor temperature</td>
</tr>
<tr>
<td>led-status</td>
<td>Displays LED state variables and the current state</td>
</tr>
<tr>
<td>psu</td>
<td>Displays power supply information</td>
</tr>
<tr>
<td>stats</td>
<td>Displays fan speed and sensor temperature statistics</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Displays diagnostic statistics for a specified device. If no device is specified, the system displays information for the logged device.</td>
</tr>
<tr>
<td><strong>service show guest-registration</strong></td>
<td>Displays status of the guest-registration database snapshot related processes (export, import, and restore)</td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code></td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><strong>export-status</strong></td>
<td>Displays the status of the latest export process initiated</td>
</tr>
<tr>
<td><strong>import-status</strong></td>
<td>Displays the status of the latest import process initiated</td>
</tr>
<tr>
<td><strong>export-status</strong></td>
<td>Displays the status of the latest restore process initiated</td>
</tr>
<tr>
<td><strong>service show fast-switching</strong></td>
<td>Displays fast switching state (enabled or disabled)</td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code></td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>**service show fib</td>
<td>fib6**</td>
</tr>
<tr>
<td><code>&lt;table-id &lt;0-255&gt;</code></td>
<td>FIB is a collection of routing entries. A route entry consists of IPv6 network (which can also be a host address, the prefix length for the network (for IPv6 routes this is between 0 - 128), and the next hop’s (gateway) IPv6 address. Since a destination can be reached through multiple next hops, you can configure multiple routes to the same destination with multiple next hops.</td>
</tr>
<tr>
<td><strong>service show mint</strong></td>
<td>Displays MiNT protocol details</td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code></td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| adopted-devices on `<DEVICE-NAME>` | Displays adopted devices status in dpd2  
  - on `<DEVICE-NAME>` – Optional. Displays MiNT protocol details for a specified device. If no device is specified, the system displays information for the logged device.  
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |
| ports | Displays MiNT ports used by various services and features |
| `service show pm {history} {(on <DEVICE-NAME>)}` | |
| `service show rf-domain-manager [diag|info] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}` | Displays RF Domain manager information  
  - `<MAC/HOSTNAME>` Optional. Specify the MAC address or hostname of the RF Domain manager.  
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
| `service show sites` | Displays NOC sites related information |
| `service show virtual-machine-history {on <DEVICE-NAME>}` | Displays virtual machine history based on the passed parameters  
  **Note:** This command is applicable only to the NX45XX, NX65XX, and NX9500, and NX9510 series service platforms. It is also available on the Privilege Executable Mode of these devices.  
  - `<DEVICE-NAME>` – Specify the name of the service platform. |
- **service show wireless [aaa-stats|adaptivity-status|credential-cache|dns-cache|radar-status|vlan-usage] \{on <DEVICE-NAME>\}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>wireless</td>
<td>Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)</td>
</tr>
<tr>
<td>aaa-stats</td>
<td>Displays AAA policy statistics</td>
</tr>
<tr>
<td>adaptivity-status</td>
<td>Displays the current list of channels (with interference levels exceeding the configured threshold resulting in adaptivity kicking in) and time when adaptivity kicked in on a device</td>
</tr>
<tr>
<td>credential-cache</td>
<td>Displays clients cached credentials statistics (VLAN, keys etc.)</td>
</tr>
<tr>
<td>dns-cache</td>
<td>Displays cache of resolved names of servers related to wireless networking</td>
</tr>
</tbody>
</table>
| radar-status | Displays radar discovery status. This option displays following information:  
• If a radar has been discovered by the AP  
• The time of discovery |
| vlan-usage | Displays VLAN statistics across WLANs |
| on <DEVICE-NAME> | The following keywords are common to all of the above:  
• on <DEVICE-NAME> – Optional. Displays running system statistics on a specified device. If no device is specified, the system displays information for the logged device.  
• <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- **service show wireless [config-internal|log-internal|neighbors]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| show     | Displays running system statistics based on the parameters passed  
**Note:** This command is not supported on the NX45XX, NX65XX, and NX9000 series service platforms. |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.) |
| config-internal | Displays internal configuration parameters |
| log-internal | Displays recent internal wireless debug logs (info and above severity) |
| neighbors | Displays neighboring device statistics for roaming and flow migration |

- **service show wireless [client|meshpoint neighbor] proc [info|stats] \{<MAC>\} \{on <DEVICE-OR-DOMAIN-NAME>\}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>wireless</td>
<td>Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)</td>
</tr>
<tr>
<td>client</td>
<td>Displays WLAN client statistics</td>
</tr>
<tr>
<td>meshpoint neighbor</td>
<td>Displays meshpoint related proc entries</td>
</tr>
</tbody>
</table>
### COMMON COMMANDS

| proc | The following keyword is common to client and meshpoint neighbor parameters:
|      | • proc – Displays dataplane proc entries based on the parameter selected
|      | **Note:** These proc entries provide statistics on each wireless client on the WLAN.
|      | **Note:** For the meshpoint parameter, it displays proc entries about neighbors.
| info | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain
| stats | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain
| <MAC> | Displays information for a specified device (wireless client or neighbor) or RF Domain
| on <DEVICE-OR-DOMAIN-NAME> | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain.
|      | • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- service show wireless radio-internal [radio1|radio2] <LINE>

| show | Displays running system statistics based on the parameters passed
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.)
| radio-internal | Displays radio internal debug logs. Select the radio from the following options:
|      | • radio1 – Selects radio 1
|      | • radio2 – Selects radio 2.
| <LINE> | Specify the radio internal debug command to enable.

- service show wireless reference [channels|frame|handshake|mcs-rates|reason-codes|status-codes]

| show | Displays running system statistics based on the parameters passed
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.)
| reference | Displays look up reference information related to standards, protocols etc.
| channels | Displays 802.11 channels information
| frame | Displays 802.11 frame structure
| handshake | Displays a flow diagram of 802.11 handshakes
| mcs-rates | Displays MCS rate information
| reason-codes | Displays 802.11 reason codes (for deauthentication, disassociation etc.)
| status-codes | Displays 802.11 status codes (for association response etc.)

- service show wireless stats-client diag {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}

| show | Displays running system statistics based on the parameters passed
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.)
| stats-client | Displays managed AP statistics
### smart-rf

Enables Smart RF management

<table>
<thead>
<tr>
<th><strong>clear-config</strong></th>
<th>Clears WLAN Smart RF configuration on a specified device or on all devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;MAC&gt;</strong></td>
<td>Optional. Clears WLAN Smart RF configuration on a device identified by its MAC address. Specify the device’s MAC address in the AA-BB-CC-DD-EE-FF format.</td>
</tr>
<tr>
<td><strong>&lt;DEVICE-NAME&gt;</strong></td>
<td>Optional. Clears WLAN Smart RF configuration on a device identified by its hostname. Specify the device’s hostname.</td>
</tr>
<tr>
<td><strong>on &lt;DOMAIN-NAME&gt;</strong></td>
<td>Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain</td>
</tr>
</tbody>
</table>

- service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}

### SNMP

Customizes a new sysObjectID (sysoid), in the MIB, for devices running WiNG 5.X devices

<table>
<thead>
<tr>
<th><strong>snmp sysoid wing5</strong></th>
<th>Configures a new sysObjectID (sysoid), in the MIB, for devices running WiNG 5.X devices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When configured, the SNMP manager returns sysoid for WiNG 5.X OS. Hardwares running the WiNG 4.X and WiNG 5.X images have different sysoids. For example, the sysoid for a RFS4000 using the WiNG 4.X image differs from another RFS4000 running the WiNG 5.X image.</td>
</tr>
<tr>
<td></td>
<td>This command is applicable only to RFS4000, RFS6000, and RFS7000 platforms, since they have the same sysoid supported in WiNG 4.X and WiNG 5.X.</td>
</tr>
<tr>
<td></td>
<td>The WiNG 4.X sysoids are:</td>
</tr>
<tr>
<td></td>
<td>• RFS4000 – 1.3.6.1.4.1.388.18</td>
</tr>
<tr>
<td></td>
<td>• RFS6000 – 1.3.6.1.4.1.388.16</td>
</tr>
<tr>
<td></td>
<td>• RFS7000 – 1.3.6.1.4.1.388.15</td>
</tr>
<tr>
<td></td>
<td>The WiNG 5.X sysoids are:</td>
</tr>
<tr>
<td></td>
<td>• RFS4000 – 1.3.6.1.4.1.388.50.1.1.35</td>
</tr>
<tr>
<td></td>
<td>• RFS6000 – 1.3.6.1.4.1.388.50.1.1.36</td>
</tr>
<tr>
<td></td>
<td>• RFS7000 – 1.3.6.1.4.1.388.50.1.1.37</td>
</tr>
</tbody>
</table>
### COMMON COMMANDS

**service ssm dump-core-snapshot**

| ssm dump-core-snapshot | Triggers a debug core dump of the SSM module |

**service syslog test {level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]} {(on <DEVICE-NAME>)}**

| syslog test | Sends a test message to the syslog server to confirm server availability |
| level | Optional. Sets the logging level. In case syslog server is unreachable, an event is logged based on the logging level defined. This is an optional parameter, and the system configures default settings, if no logging severity level is specified. |
| <0-7> | Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows: |
| alerts | Immediate action needed (severity=1) |
| critical | Critical conditions (severity=2) |
| debugging | Debugging messages (severity=7) |
| emergencies | System is unusable (severity=0) |
| errors | Error conditions (severity=3) |
| informational | Informational messages (severity=6) |
| notifications | Normal but significant conditions (severity=5) |
| warnings | Warning conditions (severity=4). This is the default setting. |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device |
| <DEVICE-NAME> | Specify the name of the AP, wireless controller, or service platform. |

**service ssm trace pattern <WORD> {on <DEVICE-NAME>**

| ssm trace | Displays the SSM module trace based on parameters passed |
| pattern <WORD> | Configures the pattern to match |
| <WORD> | Specify the pattern to match. |
| on <DEVICE-NAME> | Optional. Displays the SSM module trace on a specified device |
| <DEVICE-NAME> | Specify the name of the AP, wireless controller, or service platform. |


| wireless client beacon-requests | Sends beacon measurement requests to a wireless client |
| <MAC> | Specify the wireless client’s MAC address. |
| mode [active|passive|table] | Specifies the beacon measurement mode. The following modes are available: |
| active | Requests beacon measurements in the active mode |
| passive | Requests beacon measurements in the passive mode |
| table | Requests beacon measurements in the table mode |
| ssid [<SSID>|any] | Specifies if the measurements have to be made for a specified SSID or for any SSID |
| <SSID> | Requests beacon measurement for a specified SSID |
| any | Requests beacon measurement for any SSID |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device |
| <DEVICE-NAME> | Specify the name of the AP, wireless controller, or service platform. |
## channel-report

- **<CHANNEL-LIST>**
  - Configures channel report in the request. The request can include a list of channels or can apply to all channels.
  - **<CHANNEL-LIST>** – Request includes a list of channels. The client has to send beacon measurements only for those channels included in the request
  - **none** – Request applies to all channels

- **on <DEVICE-NAME>**
  - Optional. Sends requests on a specified device
  - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

### service wireless client quiet-element [start|stop]

<table>
<thead>
<tr>
<th>wireless client quiet-element</th>
<th>Enables the quite-element information in beacons sent to wireless clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Enables the quite-element information in beacons sent to wireless clients. This is the interval for which all wireless clients are to remain quiet.</td>
</tr>
<tr>
<td>stop</td>
<td>Disables the quite-element information in beacons sent to wireless clients. Once disabled, this information is no longer included in beacons.</td>
</tr>
</tbody>
</table>

### service wireless client trigger-bss-transition

- **mac <MAC>**
  - Specifies the wireless client’s MAC address

- **timeout <0-65535>**
  - Specifies the time remaining, for this client, before BSS transition is initiated. In other words on completion of the specified time period, BSS transition is triggered.
  - **<0-65535>** – Specify a time from 0 - 65535 seconds.

- **url <URL>**
  - Optional. Specifies session termination URL

- **on <DEVICE-OR-DOMAIN-NAME>**
  - Optional. Sends request on a specified device
  - **<DEVICE-OR-DOMAIN-NAME>** – Specify the name of the AP, wireless controller, service platform, or RF Domain.

### service wireless client trigger-wnm

- **mac <MAC>**
  - Specifies the wireless client’s MAC address

- **type [deauth-imminent|subscription-remediation]**
  - Configures the WNM notification type
  - **deauth-imminent** – Sends a de-authentication imminent frame
  - **subscription-remediation** – Sends a subscription remediation needed frame

- **uri <WORD>**
  - Optional. Specifies the unique resource identifier (URI)

### service wireless dump-core-snapshot

- **wireless client dump-core-snapshot**
  - Triggers a debug core dump of the wireless module
### Service Wireless Meshpoint ZL

Triggers a zonal level debug of a specified meshpoint’s modules

**<MESHPOINT-NAME>**
Specify the meshpoint name

**on <DEVICE-NAME>**
Triggers zonal level debug of a specified meshpoint’s modules on a specified device
- **<DEVICE-NAME>** – Specify the name of the device (AP, wireless controller, or service platform)

**<ARGS>**
Optional. Specifies the zonal arguments. These zonal arguments represent the meshpoint modules identified by the zonal and subzonal arguments passed here. Also specify the debug level from 0 - 7. Please see the *Examples* section, at the end of this topic, for more information.

**timeout <1-65535>**
Optional. Specifies a timeout value from 1 - 65535 seconds. When specified, meshpoint logs are debugged for the time specified here.

### Service Wireless QoS Delete-TSpec

Sends a delete TSPEC request to a wireless client

**<MAC>**
Specify the MAC address of the wireless client.

**tid <0-7>**
Deletes the Traffic Identifier (TID)
- **<0-7>** – Select the TID from 0 - 7.

### Service Wireless Trace Pattern

Displays the wireless module trace based on parameters passed

**pattern <WORD>**
Configures the pattern to match
- **<WORD>** – Specify the pattern to match.

**on <DEVICE-NAME>**
Optional. Displays the wireless module trace on a specified device
- **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

### Service Wireless Unsanctioned AP Air-Terminate

Enables unsanctioned access points termination

**<MAC>**
Configures the unsanctioned access points’ BSSID (MAC address)

**on <DOMAIN-NAME>**
Optional. Specifies the RD Domain of the access point
- **<DOMAIN-NAME>** – Specify the name of the RF Domain.

### Service Wireless WIPS Clear-Client-Blacklist

Enables management of WIPS parameters

**all| mac <MAC>**

clear-client-blacklist  
[all|mac <MAC>]  
Removes a specified client or all clients from the blacklist  
• all – Removes all clients from the blacklist  
• mac <MAC> – Removes a specified client form the blacklist  
• <MAC> – Specify the wireless client’s MAC address.

- service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}

wireless wips  Enables WIPS management

clear-event-history  Clears event history

on <DEVICE-OR-DOMAIN-NAME>  Optional. Clears event history on a device or RF Domain  
• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller,  
  service platform, or RF Domain.

Syntax (Privilege Exec Mode)

NOTE: The "service" command of the Priv Exec Mode is the same as the  
service command in the User Exec Mode. There a few modifications that have  
been documented in this section. For the syntax and parameters of the other  
commands refer to the (User Exec Mode) syntax and (User Exec Mode)  
parameters sections of this chapter.

service

service [block-adopter-config-updates|clear|cli-tables-skin|cluster|copy|  
delete|delete-offline-aps|force-send-config|force-update-vm-stats|  
guest-registration|load-balancing|locator|mint|pktcap|pm|radio|radius|r  
equest-full-config-from-adopter|restore|set|show|signal|smart-rf|snmp|ssm|  
start-shell|syslog|trace|wireless]

service clear crash-info {on <DEVICE-NAME>}

service copy [stats-report|tech-support]

service copy stats-report [global rf-domain <DOMAIN-NAME>] (<FILE>|<URL>)

service copy tech-support [<FILE>|<URL>]

service delete sessions <SESSION-COOKIES>

service mint [clear|debug-log|expire|<file>]

service mint [clear [lsp-db|mlcp]|debug-log [flash-and-syslog|flash-only]|  
  expire [lsp|spf] [flash [csnp|lsp]]

service pktcap on [bridge|deny|drop|ext-vlan|interface|radio|rim|router|vpn|wireless]  
{[acl-name <ACL>, count <1-1000000>, direction [any|inbound|outbound], filter <LINE>,  
  hex, rate <1-100>, snap <1-1000000>, tcpdump, verbose, write [file|url|tzsp {[IP/TZSP-  
  HOSTNAME]}]]}

service pktcap on interface [INTERFACE-NAME] [ge 1-4]|mel|port-channel 1-2|  
pppoel|vlan <1-4094>|wwan1} {[acl-name <ACL>, count <1-1000000>,  
  direction [any|inbound|outbound], filter <LINE>, hex, rate <1-100>,  
  snap <1-10048>, tcpdump, verbose, write [file|url|tzsp {[IP/TZSP-HOSTNAME]}]]}

service pktcap on radio [1-1024] [all] {[acl-name <ACL>, count <1-1000000>,  
  direction [any|inbound|outbound], filter <LINE>, hex, promiscuous, rate <1-100>,  
  snap <1-10048>, tcpdump, verbose, write [file|url|tzsp {[IP/TZSP-HOSTNAME]}]]}

service pm stop {on <DEVICE-NAME>}

service restore analytics-support [<FILE>|<URL>]

service show last-passwd

service signal [abort <PROCESS-NAME>]|kill <PROCESS-NAME>]

service start-shell
service trace <PROCESS-NAME> \{summary\}

Parameters (Privilege Exec Mode)

\> service

- service copy tech-support [\<FILE\>|\<URL\>]

<table>
<thead>
<tr>
<th>copy tech-support</th>
<th>Copies extensive system information used for troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FILE&gt;</td>
<td>Specify the location to copy file.</td>
</tr>
<tr>
<td></td>
<td>usbX:/path/file</td>
</tr>
<tr>
<td></td>
<td>Note: The number of USB ports available varies with type. For example, RFS6000 has one (1) port, NX4500 has four (4) ports.</td>
</tr>
<tr>
<td>&lt;URL&gt;</td>
<td>Specify the location URL to copy file. Both IPv4 and IPv6 address formats are supported.</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;:@&lt;hostname</td>
</tr>
</tbody>
</table>

- service copy stats-report [global|rf-domain \<DOMAIN-NAME\>] (\<FILE\>|\<URL\>)

<table>
<thead>
<tr>
<th>copy stats-report</th>
<th>Copies extensive statistical data useful for troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>[global</td>
<td>rf-domain &lt;DOMAIN-NAME&gt;]</td>
</tr>
<tr>
<td></td>
<td>• global – Copies extensive statistical data of all configured RF Domains</td>
</tr>
<tr>
<td></td>
<td>• rf-domain &lt;DOMAIN-NAME&gt; – Copies extensive statistical data of a specified RF Domain. Specify the domain name.</td>
</tr>
<tr>
<td>&lt;FILE&gt;</td>
<td>Specify the location to copy file</td>
</tr>
<tr>
<td></td>
<td>usbX:/path/file</td>
</tr>
<tr>
<td></td>
<td>Note: The number of USB ports available varies with device type. For example, RFS6000 has one (1) port, NX4500 has four (4) ports.</td>
</tr>
<tr>
<td>&lt;URL&gt;</td>
<td>Specify the location URL to copy file. Both IPv4 and IPv6 address formats are supported.</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;:@&lt;hostname</td>
</tr>
</tbody>
</table>

- service clear crash-info \{on \<DEVICE-NAME\>\}

<table>
<thead>
<tr>
<th>clear crash-info</th>
<th>Clears all crash files</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears crash files on a specified device. These crash files are core, panic, and AP dump.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- service delete sessions \<SESSION-COOKIES\>

<table>
<thead>
<tr>
<th>delete sessions &lt;SESSION-COOKIES&gt;</th>
<th>Deletes session cookies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;SESSION-COOKIES&gt; – Provide a list of cookies to delete.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mint</th>
<th>Enables MiNT protocol management (clears LSP database, enables debug logging, enables running silence etc.)</th>
</tr>
</thead>
</table>
| clear [lsp-dp|mlcp] | Clears LSP database and MiNT Link Control Protocol (MLCP) links  
  - lsp-dp – Clears MiNT Label Switched Path (LSP) database  
  - mlcp – Clears MLCP links |
| debug-log [flash-and-syslog|flash-only] | Enables debug message logging  
  - flash-and-syslog – Logs debug messages to the flash and syslog files  
  - flash-only – Logs debug messages to the flash file only |
| expire [lsp|spf] | Forces expiration of LSP and recalculation of Shortest Path First (SPF)  
  - lsp – Forces expiration of LSP  
  - spf – Forces recalculation of SPF |
| flood [csnp|lsp] | Floods control packets  
  - csnp – Floods our Complete Sequence Number Packets (CSNP)  
  - lsp – Floods our LSP |

• **service pm stop {on <DEVICE-NAME>}**

<table>
<thead>
<tr>
<th>pm</th>
<th>Stops the Process Monitor (PM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>stop</td>
<td>Stop the PM from monitoring all daemons</td>
</tr>
</tbody>
</table>
| on <DEVICE-NAME> | Optional. Stops the PM on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• **service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless]  
  {(acl-name <ACL>, count <1-1000000>, direction [any|inbound|outbound], filter, hex,  
  rate <1-100>, snap <1-2048>, tcpdump, verbose, write [file|url|tzsp <IP/TZSP-HOSTNAME>]}**

| pktcap on | Captures data packets crossing at a specified location  
  - on – Defines the packet capture location |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge</td>
<td>Captures packets transiting through the Ethernet bridge</td>
</tr>
<tr>
<td>deny</td>
<td>Captures packets denied by an Access Control List (ACL)</td>
</tr>
<tr>
<td>drop</td>
<td>Captures packets at the drop locations</td>
</tr>
<tr>
<td>ext-vlan</td>
<td>Captures packets forwarded to or from an extended VLAN</td>
</tr>
<tr>
<td>rim</td>
<td>Captures packets at the Radio Interface Module (RIM)</td>
</tr>
<tr>
<td>router</td>
<td>Captures packets transiting through an IP router</td>
</tr>
<tr>
<td>vpn</td>
<td>Captures packets forwarded to or from a VPN link</td>
</tr>
<tr>
<td>wireless</td>
<td>Captures packets forwarded to or from a wireless device</td>
</tr>
<tr>
<td>acl-name &lt;ACL&gt;</td>
<td>Optional. Specify the ACL that matches the acl-name for the 'deny' location</td>
</tr>
<tr>
<td>count &lt;1-1000000&gt;</td>
<td>Optional. Limits the captured packet count. Specify a value from 1 -1000000.</td>
</tr>
</tbody>
</table>
### COMMON COMMANDS

**direction**
- *Optional.* Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.
- **[any|inbound|outbound]**

**filter**
- *Optional.* Filters packets based on the option selected (must be used as a last option)
- **<LINE>|arp|capwap|cdp|dot11|dropreason|dst|ether|failed|host|icmp|icmp6|igmp|ip|ipv6|l2|l3|l4|lldp|mint|net|not|port|priority|radio|rssi|src|stp|tcp|tcp6|udp|udp6|vlan|wlan**
- The filter options are:
  - `<LINE>` – Defines user defined packet capture filter
  - `arp` – Matches ARP packets
  - `capwap` – Matches CAPWAP packets
  - `cdp` – Matches CDP packets
  - `dot11` – Matches 802.11 packets
  - `dropreason` – Matches packet drop reason
  - `dst` – Matches IP destination
  - `ether` – Matches Ethernet packets
  - `failed` – Matches failed 802.11 transmitted frames
  - `host` – Matches host destination
  - `icmp` – Matches ICMP packets
  - `icmp6` – Matches ICMPv6 frames
  - `ip` – Matches IPV4 packets
  - `ipv6` – Matches IPV6 packets
  - `l2` – Matches L2 header
  - `l3` – Matches L3 header
  - `l4` – Matches L4 header
  - `lldp` – Matches LLDP packets
  - `mint` – Matches MiNT packets
  - `net` – Matches IP in subnet
  - `not` – Filters out any packet that matches the filter criteria (For example, if not TCP is used, all tcp packets are filtered out)
  - `port` – Matches TCP or UDP port
  - `priority` – Matches packet priority
  - `radio` – Matches radio
  - `rssi` – Matches Received Signal Strength Indication (RSSI) of received radio signals
  - `src` – Matches IP source
  - `stp` – Matches STP packets
  - `tcp` – Matches TCP packets
  - `tcp6` – Matches TCP over IPv6 packets
  - `udp` – Matches UDP packets
  - `udp6` – Matches UDP over IPv6 packets
  - `vlan` – Matches VLAN
  - `wlan` – Matches WLAN

**hex**
- *Optional.* Provides binary output of the captured packets

**rate <1-100>**
- *Optional.* Specifies the packet capture rate
  - `<1-100>` – Specify a value from 1 - 100 seconds.

**snap <1-2048>**
- *Optional.* Captures the data length
  - `<1-2048>` – Specify a value from 1 - 2048 characters.
### service pktcap on radio

- `<1-1024>` – specify the radio index from 1 - 1024.
- `all` – captures data packets on all radios

#### acl-name <ACL>

Optional. Specify the ACL that matches the ACL name for the 'deny' location

#### count <1-1000000>

Optional. Sets a specified number of packets to capture
- `<1-1000000>` – Specify a value from 1 - 1000000.

#### direction

- `[any|inbound|outbound]` – changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.

#### filter <LINE>

Optional. Filters packets based on the option selected (must be used as a last option)
- `<LINE>` – Define a packet capture filter or select any one of the available options.

#### hex

Optional. Provides binary output of the captured packets

#### rate `<1-100>`

Optional. Specifies the packet capture rate
- `<1-100>` – Specify a value from 1 - 100 seconds.

#### snap `<1-2048>`

Optional. Captures the data length
- `<1-2048>` – Specify a value from 1 - 2048 characters.

#### tcpdump

Optional. Decodes the TCP dump

#### verbose

Optional. Provides verbose output
| write | Captures packets to a specified file. Specify the location to capture file:  
  FILE – flash:/path/file  
  usbX:/path/file  
  nvram:startup-config  
  Note: The number of USB ports available varies with type. For example, RFS6000 has one (1) port, NX4500 has four (4) ports.  
  URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.  
  tftp://<hostname|IPv4/IPv6>[:port]/path/file  
  ftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]/path/file  
  sftp://<user>@<hostname|IPv4/IPv6>[:port]/path/file  
  tzsp – The TZSP host. Specify the TZSP host's IP address or hostname. |
|------------------|----------------------------------------------------------------------------------|
| service pktcap on interface [<INTERFACE>|ge <1-4>|me|port-channel <1-2>|vlan <1-4094>] | Captures data packets at a specified interface  
  on – Specify the capture location. |
| interface [<INTERFACE>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>] | Captures packets at a specified interface. The options are:  
  • <INTERFACE> – Specify the interface name.  
  • ge <1-4> – Selects a GigabitEthernet interface index from 1 - 4  
  • me1 – Selects the FastEthernet interface  
  • port-channel <1-2> – Selects a port-channel interface index from 1 - 2  
  • vlan <1-4094> – Selects a VLAN ID from 1 - 4094 |
| acl-name <ACL> | Optional. Specify the ACL that matches the ACL name for the 'deny' location |
| count <1-1000000> | Optional. Sets a specified number of packets to capture  
  • <1-1000000> – Specify a value from 1 - 1000000. |
| direction [any|inbound|outbound] | Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound. |
| filter <LINE> | Optional. Filters packets based on the option selected (must be used as a last option)  
  • <LINE> – Define a packet capture filter or select any one of the available options. |
| hex | Optional. Provides binary output of the captured packets |
| rate <1-100> | Optional. Specifies the packet capture rate  
  • <1-100> – Specify a value from 1 - 100 seconds. |
| snap <1-2048> | Optional. Captures the data length  
  • <1-2048> – Specify a value from 1 - 2048 characters. |
| tcpdump | Optional. Decodes the TCP dump |
| verbose | Optional. Provides verbose output |
service show last-passwd

show Displays running system statistics based on the parameters passed

last-passwd Displays the last password used to enter shell

• service signal [abort <PROCESS-NAME> | kill <PROCESS-NAME>]

signal Sends a signal to a process
  • tech-support – Copies extensive system information useful for troubleshooting

abort Sends an abort signal to a process, and forces it to dump to core
  • <PROCESS-NAME> – Specify the process name.

kill Sends a kill signal to a process, and forces it to terminate without a core
  • <PROCESS-NAME> – Specify the process name.

• service start-shell

start-shell Provides shell access

• service trace <PROCESS-NAME> {summary}

trace Traces a process for system calls and signals

<PROCESS-NAME> Specifies the process name

summary Optional. Generates summary report of the specified process

Syntax (Privilege Exec Mode: NX9000, NX9500, and NX9510)

service

The following service commands are specific to the NX9000, NX9500, and NX9510 series service platforms:

service copy analytics-support [ <FILE> | <URL> ]

Parameters (Privilege Exec Mode: NX9000, NX9500, and NX9510)

• service copy analytics-support [ <FILE> | <URL> ]

copy analytics-support Enables copying of analytics information to a specified. Use one of the following options to specify the file:

  Note: This information is useful to troubleshoot issues by the Technical Support team.
Usage Guidelines
The NX9500 and NX9510 model service platforms (NOC) provide granular and robust analytic reporting for a RFS4000, RFS6000, RFS7000, NX45XX, or NX65XX device managed network. The data analyzed is collected at intervals specified by the administrator.

To enable data analytics, procure and apply a separate hot spare analytics license at the NOC. The license restricts the number of access point streams processed at the NOC or forwarded to partner systems for further processing. The analytics feature can be turned on at select APs by enabling them in configuration. This way the customer can enable analytics on a select set of APs and not the entire system as long as the number of APs on which it is enabled is less than or equal to the total number of AP analytics licenses available at the NOC controller.

In an NOC managed network, the analytics engine parses and processes Smart RF events as they are received. The analytics engine parses the new channel and power information from the Smart RF event, as opposed to retrieving the event from the devices themselves.

Syntax (Global Config Mode)

service

service [set|show cli]

service set [command-history <10-300>|upgrade-history <10-100>|reboot-history <10-100]|virtual-machine-history <10-200> {on <DEVICE-NAME>}

service show cli

Parameters (Global Config Mode)

- service set [command-history <10-300>|upgrade-history <10-100>]
  
- reboot-history <10-100]|virtual-machine-history <10-200> {on <DEVICE-NAME>}

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the size of history files</td>
</tr>
<tr>
<td>command-history &lt;10-300&gt;</td>
<td>Sets the size of the command history file</td>
</tr>
<tr>
<td>upgrade-history &lt;10-100&gt;</td>
<td>Sets the size of the upgrade history file</td>
</tr>
<tr>
<td>reboot-history &lt;10-100&gt;</td>
<td>Sets the size of the reboot history file</td>
</tr>
<tr>
<td>virtual-machine-history &lt;10-200&gt;</td>
<td>Sets the size of the virtual-machine history file</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Sets the size of history files on a specified device</td>
</tr>
</tbody>
</table>

Note: This command is applicable only to the NX45XX, NX65XX, NX9500, and NX9510 series service platforms. Use the no > service > set > virtual-machine-history > {on <DEVICE-NAME>} command to revert the history file size to 100.

Example:

```
set command-history 200
```
service show cli

show cli Displays running system configuration details
  • cli – Displays the CLI tree of the current mode

Examples
rfs7000-37FABE>service cli-tables-skin stars
rfs7000-37FABE>service show cli
Command mode: +-do
  +-help [help]
  +-search
    +-WORD [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-detailed [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-only-show [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-skip-show [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-skip-no [help search WORD ([detailed|only-show|skip-show|skip-no])
  +-show
    +-commands [show commands]
    +-adoption
      +-log
        +-adoptee [show adoption log adoptee([on DEVICE-NAME])
        +-on
          +-DEVICE-NAME [show adoption log adoptee([on DEVICE-NAME])
        +-adopter [show adoption log adopter ([mac AA-BB-CC-DD-EE-FF](|on DEVICE-NAME))
          +-mac
            +-AA-BB-CC-DD-EE-FF [show adoption log adopter ([mac AA-BB-CC-DD-EE-FF](|on DEVICE-NAME))
            +-on
              +-DEVICE-NAME [show adoption log adopter ([mac AA-BB-CC-DD-EE-FF](|on DEVICE-NAME))
--More--
rfs7000-37FABE>
rfs7000-37FABE#service signal abort testprocess
Sending an abort signal to testprocess
rfs7000-37FABE#
rfs7000-37FABE#service pm stop
rfs7000-37FABE#
rfs7000-37FABE(config)#service show cli
Global configuration mode:
  +-help [help]
  +-search
    +-WORD [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-detailed [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-only-show [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-skip-show [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-skip-no [help search WORD ([detailed|only-show|skip-show|skip-no])
  +-show
    +-commands [show commands]
    +-adoption
      +-log
        +-adoptee [show adoption log adoptee([on DEVICE-NAME])
        +-on
          --More--
rfs7000-37FABE(config)#
rfs4000-229D58>service show command-history
Configured size of command history is 200

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>User</th>
<th>Location</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 01 08:54:41 2015</td>
<td>admin</td>
<td>192.168.100.138 16</td>
<td>reload force</td>
</tr>
<tr>
<td>May 26 08:37:15 2015</td>
<td>admin</td>
<td>192.168.100.120 17</td>
<td>reload force</td>
</tr>
<tr>
<td>May 26 08:37:15 2015</td>
<td>admin</td>
<td>192.168.100.120 17</td>
<td>write memory</td>
</tr>
<tr>
<td>May 18 08:31:17 2015</td>
<td>admin</td>
<td>192.168.100.214 15</td>
<td>reload force</td>
</tr>
<tr>
<td>May 11 08:23:04 2015</td>
<td>admin</td>
<td>192.168.100.209 13</td>
<td>reload force</td>
</tr>
<tr>
<td>May 06 11:04:47 2015</td>
<td>admin</td>
<td>192.168.100.239 11</td>
<td>reload force</td>
</tr>
<tr>
<td>May 04 09:19:42 2015</td>
<td>admin</td>
<td>192.168.100.197 8</td>
<td>reload force</td>
</tr>
<tr>
<td>May 04 09:19:42 2015</td>
<td>admin</td>
<td>192.168.100.197 8</td>
<td>write memory</td>
</tr>
<tr>
<td>Apr 24 10:07:30 2015</td>
<td>admin</td>
<td>192.168.100.238 11</td>
<td>reload force</td>
</tr>
<tr>
<td>Apr 24 10:07:30 2015</td>
<td>admin</td>
<td>192.168.100.238 11</td>
<td>write memory</td>
</tr>
<tr>
<td>Apr 23 16:50:51 2015</td>
<td>admin</td>
<td>192.168.100.208 10</td>
<td>revert</td>
</tr>
<tr>
<td>Apr 23 16:42:16 2015</td>
<td>admin</td>
<td>192.168.100.208 10</td>
<td>clear event-history</td>
</tr>
<tr>
<td>Apr 16 03:56:50 2015</td>
<td>admin</td>
<td>192.168.100.208 19</td>
<td>reload force</td>
</tr>
<tr>
<td>Apr 08 04:42:14 2015</td>
<td>admin</td>
<td>192.168.100.183 19</td>
<td>reload force</td>
</tr>
<tr>
<td>Mar 31 06:23:08 2015</td>
<td>admin</td>
<td>192.168.100.164 10</td>
<td>interface radio 1</td>
</tr>
<tr>
<td>Mar 31 06:23:05 2015</td>
<td>admin</td>
<td>192.168.100.164 10</td>
<td>self</td>
</tr>
</tbody>
</table>

--More--
rfs4000-229D58>

rfs7000-37FABE>service show diag stats

fan 1 current speed: 6660 min_speed: 2000 hysteresis: 250
fan 2 current speed: 6720 min_speed: 2000 hysteresis: 250
fan 3 current speed: 6540 min_speed: 2000 hysteresis: 250

Sensor 1 Temperature 32.0 C
Sensor 2 Temperature 58.0 C
Sensor 3 Temperature 29.0 C
Sensor 4 Temperature 28.0 C
Sensor 5 Temperature 26.0 C
Sensor 6 Temperature 28.0 C

rfs7000-37FABE>

rfs7000-37FABE>service show info

7.9M out of 8.0M available for logs.
32.9M out of 34.0M available for history.
81.9M out of 84.0M available for crashinfo.

List of Files:

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>anald.log</td>
<td>1.3K</td>
<td>Apr 4</td>
<td>10:48</td>
</tr>
<tr>
<td>cfgd.log</td>
<td>9.7K</td>
<td>Apr 4</td>
<td>14:38</td>
</tr>
<tr>
<td>dpd2.log</td>
<td>21.4K</td>
<td>Apr 4</td>
<td>10:48</td>
</tr>
<tr>
<td>messages.log</td>
<td>0</td>
<td>Apr 4</td>
<td>10:46</td>
</tr>
<tr>
<td>startup.log</td>
<td>9.5K</td>
<td>Apr 4</td>
<td>10:48</td>
</tr>
<tr>
<td>upgrade.log</td>
<td>1.6K</td>
<td>Apr 4</td>
<td>10:50</td>
</tr>
<tr>
<td>vlan-usage.log</td>
<td>0</td>
<td>Apr 4</td>
<td>14:32</td>
</tr>
<tr>
<td>command.history</td>
<td>1.6K</td>
<td>Apr 4</td>
<td>14:37</td>
</tr>
<tr>
<td>reboot.history</td>
<td>2.1K</td>
<td>Apr 4</td>
<td>10:46</td>
</tr>
<tr>
<td>upgrade.history</td>
<td>522</td>
<td>Apr 4</td>
<td>10:45</td>
</tr>
</tbody>
</table>

Please export these files or delete them for more space.

rfs7000-37FABE>

nx9500-6C8809>service show mac-vendor B4-C7-99-6C-88-09
B4-C7-99 : Zebra Tech
nx9500-6C8809>
nx9500-6C8809>service show upgrade-history
Configured size of upgrade history is 50

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Old Version</th>
<th>New Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 01 08:48:43 2015</td>
<td>5.8.1.0-034B</td>
<td>5.8.1.0-035B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 26 08:20:46 2015</td>
<td>5.8.1.0-033B</td>
<td>5.8.1.0-034B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 18 08:26:47 2015</td>
<td>5.8.1.0-032B</td>
<td>5.8.1.0-033B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 11 08:31:28 2015</td>
<td>5.8.1.0-031B</td>
<td>5.8.1.0-032B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 11 08:17:24 2015</td>
<td>5.8.1.0-031B</td>
<td>5.8.1.0-032B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 06 10:53:54 2015</td>
<td>5.8.1.0-028D</td>
<td>5.8.1.0-031B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 06 10:45:09 2015</td>
<td>5.8.1.0-030B</td>
<td>5.8.1.0-028D</td>
<td>Successful</td>
</tr>
<tr>
<td>May 04 09:41:10 2015</td>
<td>5.8.1.0-028D</td>
<td>5.8.1.0-030B</td>
<td>Successful</td>
</tr>
<tr>
<td>May 04 09:03:26 2015</td>
<td>5.8.1.0-028D</td>
<td>5.8.1.0-028D</td>
<td>Successful</td>
</tr>
<tr>
<td>Apr 24 10:01:39 2015</td>
<td>5.8.1.0-028D</td>
<td>5.8.1.0-028D</td>
<td>Successful</td>
</tr>
<tr>
<td>Apr 23 10:43:02 2015</td>
<td>5.8.1.0-027D</td>
<td>5.8.1.0-028D</td>
<td>Successful</td>
</tr>
<tr>
<td>Apr 16 08:43:32 2015</td>
<td>5.8.1.0-025D</td>
<td>5.8.1.0-027D</td>
<td>Successful</td>
</tr>
<tr>
<td>Mar 31 08:40:17 2015</td>
<td>5.8.1.0-023D</td>
<td>5.8.1.0-025D</td>
<td>Successful</td>
</tr>
<tr>
<td>Mar 20 08:49:42 2015</td>
<td>5.8.1.0-021D</td>
<td>5.8.1.0-023D</td>
<td>Successful</td>
</tr>
</tbody>
</table>

--More--

rfs7000-37FABE#service show wireless reference reason-codes
CODE DESCRIPTION
0    Success
1    Unspecified Reason
2    Previous authentication no longer valid
3    Deauth because sending STA is leaving IBSS or ESS
4    Disassoc due to inactivity
5    Disassoc because AP is unable to handle all currently assoc STA
6    Class 2 frame received from non-authenticated STA
7    Class 3 frame received from nonassociated STA

--More--

rfs7000-37FABE#service show wireless reference status-codes
CODE DESCRIPTION
0    Successful
1    Unspecified failure
2-9  Reserved
10   Cannot support all requested capabilities in the Capability Information field
11   Reassociation denied due to inability to confirm that association exists
12   Association denied due to reason outside the scope of this standard
13   Responding STA does not support the specified authentication algorithm
14   Received an auth frame with authentication transaction seq number out of expected sequence
15   Authentication rejected because of challenge failure

--More--

rfs4000-229D58>service show xpath-history

<table>
<thead>
<tr>
<th>DATE&amp;TIME</th>
<th>USER</th>
<th>XPATH</th>
<th>DURATION(MS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Jun 5 14:16:34 2015</td>
<td>system</td>
<td>wing-stats/device/00-23-68-88-0D-A7/upgrade-history</td>
<td>16</td>
</tr>
<tr>
<td>Fri Jun 5 14:15:14 2015</td>
<td>system</td>
<td>wing-stats/stats/device/00-23-68-88-0D-A7/command-history</td>
<td>26</td>
</tr>
</tbody>
</table>

rfs4000-229D58>

rfs7000-37FABE>service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
no country-code

rfs7000-37FABE>
The following example shows the service > show > virtual-machine-history output on a NX4500 service platform:

```
nx4500-5CFA2B>service show virtual-machine-history
Configured size of virtual machine history is 100

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Virtual Machine</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 01 08:54:21</td>
<td>team-urc</td>
<td>autostart</td>
</tr>
<tr>
<td>Jun 01 08:52:54</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
<tr>
<td>May 26 08:25:25</td>
<td>team-urc</td>
<td>autostart</td>
</tr>
<tr>
<td>May 26 08:23:54</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
<tr>
<td>May 18 08:30:03</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
<tr>
<td>May 18 08:29:58</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
<tr>
<td>May 11 08:25:16</td>
<td>team-urc</td>
<td>autostart</td>
</tr>
<tr>
<td>May 11 08:23:47</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
</tbody>
</table>
```

```
nx4500-5CFA2B>service clear virtual-machine-history
```

```
nx4500-5CFA2B>service show virtual-machine-history
Configured size of virtual machine history is 100

No entries in virtual machine history
```

The following example shows the service > show > virtual-machine-history output on a NX9500 service platform:

```
nx9500-6C874D>service show virtual-machine-history
Configured size of virtual machine history is 100

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Virtual Machine</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 01 08:55:21</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 26 08:27:27</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 18 08:32:53</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 11 08:38:54</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 11 08:26:09</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 06 10:58:37</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 06 10:49:48</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>May 04 09:09:40</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Apr 24 10:06:52</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Apr 23 11:06:43</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Apr 16 08:48:55</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Mar 31 10:12:05</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
</tbody>
</table>
```

```
nx9500-6C874D>```
The following example displays the site configuration on a NOC controller:

```
nx9500-6C8809>service show sites
-- Site [B4-C7-99-5C-FA-8E] --
  [B4-C7-99-5C-FA-8E] - Controller, Adopted
  Cfg Status: configured
  [00-23-68-11-E6-C4] - AP
  [B4-C7-99-74-B4-5C] - AP
-- Site [B4-C7-99-6D-B5-D4] --
  [B4-C7-99-6D-B5-D4] - Controller, Adopted
  Cfg Status: configured
-- Site [TechPubsLan] --
  [B4-C7-99-6D-CD-4B] - Controller, Adopted, Master
  Cfg Status: configured
-- Site [B4-C7-99-6D-CD-4B] --
  [B4-C7-99-74-B4-5C] - AP
  [B4-C7-99-58-72-58] - AP
-- Site [TechPubsLAN] --
  [00-23-68-88-0D-A7] - Controller, Adopted, Master
  Cfg Status: configured
-- Site [TechPubs] --
  [00-23-68-22-9D-58] - Controller, Adopted
  Cfg Status: configured
  [B4-C7-99-5C-FA-2B] - Controller, Adopted
  Cfg Status: configured
nx9500-6C8809>
```

```
rfs7000-6DCD4B>service show sites
-- Site [B4-C7-99-6D-CD-4B] --
  [B4-C7-99-74-B4-5C] - AP
  [00-23-68-11-E6-C4] - AP
-- Site [00-15-70-81-74-2D] --
  [B4-C7-99-71-17-28] - AP
  [00-15-70-81-74-2D] - Controller, Adopted
  Cfg Status: version-mismatch
rfs7000-6DCD4B>
rfs4000-229D58#service show fib6
-------------------------------------------------------------------------------
Route Table ID : 254
::1/128          Interface: lo               Route Type: ROUTE_TYPE_CONNECT
  Route Status: ROUTE_STATUS_KERNEL  Metric: 0 Distance: 0
fe80::/64        Interface: vlan2            Route Type: ROUTE_TYPE_CONNECT
  Route Status: ROUTE_STATUS_KERNEL  Metric: 256 Distance: 0
2001::/64        Interface:                  Route Type: ROUTE_TYPE_STATIC
  Route Status: ROUTE_STATUS_PENDING Metric: 256 Distance: 1
rfs4000-229D58#
```
Examples for the `service > wireless > meshpoint` command.

The following example displays meshpoint modules:

```
ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
```

```
<table>
<thead>
<tr>
<th>SUBZONE</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-LLC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN TX RX BEA TXF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-ND</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN TX RX NBR LQM LSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-ORL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-LQ</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-PS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7-RS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-IA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11-MGT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN RX TX R0 LMST LSUP LKEY KEY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13-LSA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN SCAN TRIG</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14-ACS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15-EAP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16-L2P</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

In the preceding example,

- The meshpoint name is `mesh_root`
- The device on which the command is executed is `ROOT1-ap81xx-71174C`
- The vertical `ZONE` column represents meshpoint modules. For example, `3-ND` presents the Neighbor Discovery module.
- The `SUBZONE` 0 to 7 represents the available processes for each of the zonal modules.
- Debugging is disabled for all modules for the mesh-root meshpoint. A value of 0 (Zero) represents debugging disabled.
To enable meshpoint module debugging, specify the module number and the process number separated by a period (.) And then specify the debugging level from 0 - 7.

ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C 3.2 7

In the preceding command,
- The meshpoint module number provided is 3 (ND)
- The process number provided is 2 (RX - Received signals from neighbors)
- The debugging level provided is 7 (highest level - warning)

ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C

| SUBZONE | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
---|---|---|---|---|---|---|---|---|
| ZONE | GEN | TX | RX | BEA | TXF |
| 2-LLC | 0 | 0 | 0 | 0 | 0 |
| 3-ND | 0 | 0 | 7(D) | 0 | 0 | 0 |
| 4-ORL | 0 | GEN | TX | RX | HEL | PRO |
| 5-LQ | 0 | 0 | 0 | 0 | 0 |
| 6-PS | 0 | GEN | ROOT | NBR | REC |
| 7-RS | 0 | 0 | 0 | 0 |
| 8-IA | 0 | GEN | SET | GET |
| 11-MGT | 0 | 0 | 0 |
| 13-LSA | GEN | RX | TX | R0 | LMST | LSUP | LKEY | KEY |
| 14-ACS | GEN | SCAN | TRIG |
| 15-EAP | 0 | GEN |
| 16-L2P | 0 |

In the preceding example, level 7 debugging has been enabled only for the ND module’s received signals. Note that debugging for all other modules and processes are still disabled.

To disable debugging for all modules, specify 0 (zero) in the command. For example:

ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C 0
To enable debugging for all modules, specify the debugging level number. For example:

```
ROOT1-ap81xx-71174C# service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C 5
```

```
<table>
<thead>
<tr>
<th>ZONE</th>
<th>GEN TX RX BEA TXF</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-LLC</td>
<td>5(N) 5(N) 5(N) 5(N) 5(N)</td>
</tr>
<tr>
<td>3-ND</td>
<td>GEN TX RX NBR LQM LSA</td>
</tr>
<tr>
<td>4-ORL</td>
<td>GEN 5(N)</td>
</tr>
<tr>
<td>5-LQ</td>
<td>GEN RX TX HEL PRO 5(N) 5(N) 5(N) 5(N) 5(N)</td>
</tr>
<tr>
<td>6-PS</td>
<td>GEN 5(N)</td>
</tr>
<tr>
<td>7-RS</td>
<td>GEN ROOT NBR REC</td>
</tr>
<tr>
<td>8-IA</td>
<td>GEN 5(N)</td>
</tr>
<tr>
<td>11-MGT</td>
<td>GEN SET GET 5(N) 5(N)</td>
</tr>
<tr>
<td>13-LSA</td>
<td>GEN RX TX R0 LMST LSUP LKEY KEY 5(N) 5(N) 5(N) 5(N) 5(N) 5(N)</td>
</tr>
<tr>
<td>14-ACS</td>
<td>GEN 5(N) 5(N)</td>
</tr>
<tr>
<td>15-EAP</td>
<td>GEN 5(N)</td>
</tr>
<tr>
<td>16-L2P</td>
<td>GEN 5(N)</td>
</tr>
</tbody>
</table>
```

```
rfs4000-1BE644# service show ssh-authorized-keys
'zebra@zebra-quadcore'
rfs4000-1BE644#
```

```
rfs4000-1BE644# service load-ssh-autorized-keys "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDPERY9aTibRY1FMnERTYP2iyyJ00YE1lxjUElY7Zm9Ky2yeSmg15UKerJ +1P161Gdm0AoEfyxeheRntK+Z6NWHa341RWJ0UrQMc7hSEE5jbDpLKJ0uEoW22Ag45B2zMV7EnM7lHowboNsQh SzX5uBB1Vv1WbxBqDroX4BcuB/ CFugezHTt95UQ2ZRUvHveP6jQdQArFlavlwk0S1csz24HNSL5DKutJ4VY+6vRvlf5Gy/ 3GNeMwNsmsRKK4UVKV5pnuUIjkbZf+goPFaKvVPNzNgjaOyDfVNGE7JIwmYlti/ AId6tv2zAbMqSomNAgU00hKXS9m4m74PnPPr zebra@zebra-quadcore"
Successfully added the ssh key
```

```
rfs4000-1BE644# no service load-ssh-autorized-keys
Successfully removed the ssh key
```

```
rfs4000-1BE644# garbage collect
```

```
rfs4000-1BE644# show processes
```

```
rfs4000-1BE644# net show interface
```

```
rfs4000-1BE644# service show disks
```

```
rfs4000-1BE644# service show services
```

```
rfs4000-1BE644# service show wv
```

```
rfs4000-1BE644# show disk
```

```
rfs4000-1BE644# service show dcm
```

```
rfs4000-1BE644# service show lmp
```

```
rfs4000-1BE644# service show skr
```

```
rfs4000-1BE644# service show mesh
```

```
rfs4000-1BE644# show interface
```

```
rfs4000-1BE644# show disks
```

```
rfs4000-1BE644# show services
```

```
rfs4000-1BE644# show wv
```

```
rfs4000-1BE644# show dcm
```

```
rfs4000-1BE644# show lmp
```

```
rfs4000-1BE644# show skr
```

```
rfs4000-1BE644# show mesh
```

```
rfs4000-1BE644# show interface
```

```
rfs4000-1BE644# show disks
```

```
rfs4000-1BE644# show services
```

```
rfs4000-1BE644# show wv
```

```
rfs4000-1BE644# show dcm
```

```
rfs4000-1BE644# show lmp
```

```
rfs4000-1BE644# show skr
```

```
rfs4000-1BE644# show mesh
```

```
rfs4000-1BE644# show interface
```

```
rfs4000-1BE644# show disks
```

```
rfs4000-1BE644# show services
```

```
rfs4000-1BE644# show wv
```

```
rfs4000-1BE644# show dcm
```

```
rfs4000-1BE644# show lmp
```

```
rfs4000-1BE644# show skr
```

```
rfs4000-1BE644# show mesh
```

```
rfs4000-1BE644# show interface
```

```
rfs4000-1BE644# show disks
```

```
rfs4000-1BE644# show services
```

```
rfs4000-1BE644# show wv
```

```
rfs4000-1BE644# show dcm
```

```
rfs4000-1BE644# show lmp
```

```
rfs4000-1BE644# show skr
```

```
rfs4000-1BE644# show mesh
```

```
rfs4000-1BE644# show interface
```

```
rfs4000-1BE644# show disks
```

```
rfs4000-1BE644# show services
```

```
rfs4000-1BE644# show wv
```

```
rfs4000-1BE644# show dcm
```

```
rfs4000-1BE644# show lmp
```

```
rfs4000-1BE644# show skr
```

```
rfs4000-1BE644# show mesh
```
5.1.8 show

Common Commands

Displays specified system component settings. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display parameter, it displays information about that component.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX5650, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```sh
show <PARAMETERS>
```

Parameters

- `show <PARAMETERS>`

The show command displays configuration details based on the configuration mode, in which the command is executed, and the parameters passed. For example, when executed in the AAA policy configuration mode, it displays the logged AAA policy’s current settings. The example below shows the configuration details that can be viewed in the Priv Executable mode.

Examples

```sh
rfs7000-37FABE#show ?
adoption Display information related to adoption to wireless controller
bonjour Bonjour Gateway related commands
boot Display boot configuration.
captive-portal Captive portal commands
captive-portal-page-upload Captive portal advanced page upload
cdp Cisco Discovery Protocol
classify-url Query the category of an URL
clock Display system clock
cluster Cluster Protocol
cmp-factory-certs Display the CMP certificate status
commands Show command lists
context Information about current context
critical-resources Critical Resources
crypto Encryption related commands
dev unsigned Debugging functions
dev unsigned Debugging functions
device-upgrade Device Upgrade
dot1x 802.1X
dpi Deep Packet Inspection
environmental-sensor Display Environmental Sensor Module status
event-history Display event history
event-system-policy Display event system policy
ex3500 EX3500 device details
extdev External device (T5, Ex3500..)
file Display filesystem information
file-sync File sync between controller and adoptees
firewall Wireless Firewall
global Global-level information
gre Show gre tunnel info
interface Interface Configuration/Statistics commands
ip Internet Protocol (IP)
ip-access-list IP ACL
```
ipv6                        Internet Protocol version 6 (IPv6)
ipv6-access-list            IPV6 ACL
l2tpv3                      L2TPv3 information
ldap-agent                  LDAP Agent Configuration
licenses                    Show installed licenses and usage
lldp                        Link Layer Discovery Protocol
logging                     Show logging information
mac-access-list             MAC Access list
mac-address-table           Display MAC address table
mac-auth                    MAC authentication
mac-auth-clients            MAC authenticated clients
mint                        MiNT protocol
ntp                         Network time protocol
password-encryption         Password encryption
pppoe-client                PPP Over Ethernet client
privilege                   Show current privilege level
radius                      RADIUS statistics commands
reload                      Scheduled reload information
remote-debug                Show details of remote debug sessions
rf-domain-manager           Show RF Domain Manager selection details
role                        Role based firewall
route-maps                  Display Route Map Statistics
rtls                        RTLS Statistics
running-config              Current operating configuration
session-changes             Configuration changes made in this session
session-config              This session configuration
sessions                    Display CLI sessions
site-config-diff            Difference between site configuration on the NOC and actual site configuration
smart-rf                    Smart-RF Management Commands
spanning-tree               Display spanning tree information
startup-config              Startup configuration
t5                          T5 details
terminal                    Display terminal configuration parameters
timezone                    The timezone
traffic-shape               Display traffic shaping
upgrade-status              Display last image upgrade status
version                     Display software & hardware version
vrrp                        VRRP protocol
web-filter                  Web filter
what                        Perform global search
wireless                    Wireless commands
wwan                        Display wireless WAN Status

NOTE: For more information on the show command, see Chapter 6, SHOW COMMANDS
5.1.9 write

Common Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

write [memory|terminal]

Parameters

- write [memory|terminal]

<table>
<thead>
<tr>
<th>memory</th>
<th>Writes to the non-volatile (NV) memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal</td>
<td>Writes to the terminal</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE>write memory
[OK]
rfs7000-37FABE>
Show commands display configuration settings or statistical information. Use this command to view the current running configuration as well as the start-up configuration. The show command also displays the current context’s configuration.

This chapter describes the ‘show’ CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

This chapter also describes the ‘show’ commands in the ‘GLOBAL CONFIG’ mode. The commands can be entered in all three modes, except commands like file, IP access list statistics, MAC access list statistics, and upgrade statistics, which cannot be entered in the USER EXEC mode.

---

**NOTE:** The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
## 6.1 show commands

### SHOW COMMANDS

The following table summarizes show commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays settings for the specified system component</td>
<td>page 6-6</td>
</tr>
<tr>
<td>adoption</td>
<td>Displays information related to adoption</td>
<td>page 6-12</td>
</tr>
<tr>
<td>boot</td>
<td>Displays a device boot configuration</td>
<td>page 6-16</td>
</tr>
<tr>
<td>bonjour</td>
<td>Displays the configured Bonjour services available on local and remote sites</td>
<td>page 6-17</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Displays WLAN hotspot functions</td>
<td>page 6-18</td>
</tr>
<tr>
<td>captive-portal-page-upload</td>
<td>Displays captive portal page related information</td>
<td>page 6-20</td>
</tr>
<tr>
<td>cdp</td>
<td>Displays a Cisco Discovery Protocol (CDP) neighbor table</td>
<td>page 6-21</td>
</tr>
<tr>
<td>classify-url</td>
<td>Queries a specified global data center or a pre-configured classification server for the category of a specified URL.</td>
<td>page 6-23</td>
</tr>
<tr>
<td>clock</td>
<td>Displays the software system clock</td>
<td>page 6-24</td>
</tr>
<tr>
<td>cluster</td>
<td>Displays cluster commands</td>
<td>page 6-25</td>
</tr>
<tr>
<td>cmp-factory-certs</td>
<td>Displays factory installed CMP certificates</td>
<td>page 6-26</td>
</tr>
<tr>
<td>commands</td>
<td>Displays command list</td>
<td>page 6-27</td>
</tr>
<tr>
<td>context</td>
<td>Displays information about the current context</td>
<td>page 6-28</td>
</tr>
<tr>
<td>critical-resources</td>
<td>Displays critical resource information</td>
<td>page 6-29</td>
</tr>
<tr>
<td>crypto</td>
<td>Displays encryption mode information</td>
<td>page 6-30</td>
</tr>
<tr>
<td>database</td>
<td>Displays database-related statistics and status</td>
<td>page 6-33</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Displays device firmware upgradation information for devices adopted by a wireless controller or access point</td>
<td>page 6-34</td>
</tr>
<tr>
<td>dot1x</td>
<td>Displays dot1x information on interfaces</td>
<td>page 6-37</td>
</tr>
<tr>
<td>dpi</td>
<td>Displays statistics for all configured and canned applications</td>
<td>page 6-39</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Displays environmental sensor’s historical data (applicable only to AP8132)</td>
<td>page 6-42</td>
</tr>
<tr>
<td>event-history</td>
<td>Displays event history</td>
<td>page 6-45</td>
</tr>
<tr>
<td>event-system-policy</td>
<td>Displays event system policy configuration information</td>
<td>page 6-46</td>
</tr>
<tr>
<td>ex3500</td>
<td>Displays EX3500-related statistical data</td>
<td>page 6-47</td>
</tr>
<tr>
<td>extdev</td>
<td>Displays external device (T5 or EX3500) configuration error history</td>
<td>page 6-50</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>file</td>
<td>Displays file system information</td>
<td>page 6-51</td>
</tr>
<tr>
<td>file-sync</td>
<td>Displays file synchronization settings and status on a controller. The file-sync command syncs EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adoptee AP6522/AP6562 client-bridge access points</td>
<td>page 6-52</td>
</tr>
<tr>
<td>firewall</td>
<td>Displays wireless firewall information</td>
<td>page 6-54</td>
</tr>
<tr>
<td>global</td>
<td>Displays global information for network devices based on the parameters passed</td>
<td>page 6-58</td>
</tr>
<tr>
<td>gre</td>
<td>Displays GRE tunnel related information</td>
<td>page 6-60</td>
</tr>
<tr>
<td>guest-registration</td>
<td>Displays guest registration statistics based on the option and time entered</td>
<td>page 6-61</td>
</tr>
<tr>
<td>interface</td>
<td>Displays interface status</td>
<td>page 6-68</td>
</tr>
<tr>
<td>ip</td>
<td>Displays IP related information</td>
<td>page 6-72</td>
</tr>
<tr>
<td>ip-access-list</td>
<td>Displays IP access list statistics</td>
<td>page 6-80</td>
</tr>
<tr>
<td>ipv6</td>
<td>Displays IPv6 related information</td>
<td>page 6-82</td>
</tr>
<tr>
<td>ipv6-access-list</td>
<td>Displays IPv6 access list statistics</td>
<td>page 6-86</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Displays Layer 2 Tunnel Protocol Version 3 (L2TPV3) information</td>
<td>page 6-87</td>
</tr>
<tr>
<td>ldap-agent</td>
<td>Displays an LDAP agent’s join status (join status to a LDAP server domain)</td>
<td>page 6-90</td>
</tr>
<tr>
<td>licenses</td>
<td>Displays installed licenses and usage information</td>
<td>page 6-91</td>
</tr>
<tr>
<td>lldp</td>
<td>Displays Link Layer Discovery Protocol (LLDP) information</td>
<td>page 6-94</td>
</tr>
<tr>
<td>logging</td>
<td>Displays logging information</td>
<td>page 6-95</td>
</tr>
<tr>
<td>mac-access-list</td>
<td>Displays MAC access list statistics</td>
<td>page 6-96</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Displays MAC address table entries</td>
<td>page 6-97</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Displays details of wired ports that have MAC address-based authentication enabled</td>
<td>page 6-98</td>
</tr>
<tr>
<td>mac-auth-clients</td>
<td>Displays MAC-authenticated clients based on the parameters passed</td>
<td>page 6-100</td>
</tr>
<tr>
<td>mint</td>
<td>Displays MiNT protocol configuration commands</td>
<td>page 6-102</td>
</tr>
<tr>
<td>ntp</td>
<td>Displays Network Time Protocol (NTP) information</td>
<td>page 6-105</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Displays password encryption status</td>
<td>page 6-107</td>
</tr>
<tr>
<td>pppoe-client</td>
<td>Displays Point to Point Protocol over Ethernet (PPPoE) client information</td>
<td>page 6-108</td>
</tr>
<tr>
<td>privilege</td>
<td>Displays current privilege level information</td>
<td>page 6-109</td>
</tr>
<tr>
<td>radius</td>
<td>Displays the amount of access time consumed and the access time remaining for all guest users configured on a RADIUS server</td>
<td>page 6-110</td>
</tr>
</tbody>
</table>
### Table 6.1 Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Displays scheduled reload information</td>
<td>page 6-112</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Displays RF Domain manager selection details</td>
<td>page 6-113</td>
</tr>
<tr>
<td>role</td>
<td>Displays role-based firewall information</td>
<td>page 6-114</td>
</tr>
<tr>
<td>route-maps</td>
<td>Display route map statistics</td>
<td>page 6-115</td>
</tr>
<tr>
<td>rts</td>
<td>Displays <em>Real Time Location Service</em> (RTLS) statistics of access points</td>
<td>page 6-116</td>
</tr>
<tr>
<td>running-config</td>
<td>Displays configuration file contents</td>
<td>page 6-117</td>
</tr>
<tr>
<td>session-changes</td>
<td>Displays configuration changes made in this session</td>
<td>page 6-123</td>
</tr>
<tr>
<td>session-config</td>
<td>Displays a list of currently active open sessions on the device</td>
<td>page 6-124</td>
</tr>
<tr>
<td>sessions</td>
<td>Displays CLI sessions</td>
<td>page 6-125</td>
</tr>
<tr>
<td>site-config-diff</td>
<td>Displays the difference between site configuration available on NOC and the actual site configuration</td>
<td>page 6-126</td>
</tr>
<tr>
<td>smart-rf</td>
<td>Displays Smart RF management commands</td>
<td>page 6-127</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Displays spanning tree information</td>
<td>page 6-131</td>
</tr>
<tr>
<td>startup-config</td>
<td>Displays complete startup configuration script on the console</td>
<td>page 6-134</td>
</tr>
<tr>
<td>t5</td>
<td>Displays adopted T5 controller details. This command is applicable only on the RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, and NX9510.</td>
<td>page 6-135</td>
</tr>
<tr>
<td>terminal</td>
<td>Displays terminal configuration parameters</td>
<td>page 6-141</td>
</tr>
<tr>
<td>timezone</td>
<td>Displays timezone information for the system and managed devices</td>
<td>page 6-142</td>
</tr>
<tr>
<td>traffic-shape</td>
<td>Displays traffic-shaping related configuration details and statistics</td>
<td>page 6-143</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Displays image upgrade status</td>
<td>page 6-145</td>
</tr>
<tr>
<td>version</td>
<td>Displays a device’s software and hardware version</td>
<td>page 6-147</td>
</tr>
<tr>
<td>vrrp</td>
<td>Displays <em>Virtual Router Redundancy Protocol</em> (VRRP) protocol details</td>
<td>page 6-148</td>
</tr>
<tr>
<td>web-filter</td>
<td>Displays pre-configured, in-built Web filter options available. These options are: category (URL category), category-types, filter-level etc. This command also displays Web filter statistics and status.</td>
<td>page 6-150</td>
</tr>
<tr>
<td>what</td>
<td>Displays details of a specified search phrase</td>
<td>page 6-152</td>
</tr>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
<td>page 6-153</td>
</tr>
<tr>
<td>wwan</td>
<td>Displays the wireless WAN status</td>
<td>page 6-174</td>
</tr>
<tr>
<td>slot</td>
<td>Displays <em>Peripheral Component Interconnect</em> (PCI) express slot statistics</td>
<td>page 6-175</td>
</tr>
<tr>
<td>smart-cache</td>
<td>Displays details on the cached entry for a specific URL or all URLs</td>
<td>page 6-176</td>
</tr>
<tr>
<td>virtual-machine</td>
<td>Displays the <em>virtual-machine</em> (VM) configuration, logs, and statistics (applicable only to the NX45XX and NX65XX service platforms)</td>
<td>page 6-178</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>mirroring</td>
<td>Displays the port mirroring sessions (applicable only to the NX4524 and NX6524 service platforms)</td>
<td>page 6-181</td>
</tr>
<tr>
<td>raid</td>
<td>Displays <em>Redundant Array of Independent Disks</em> (RAID) related information, such as array status, consistency check status, and RAID log.</td>
<td>page 6-182</td>
</tr>
</tbody>
</table>
6.1.1 show

show commands

The show command displays following information:

- A device’s current configuration
- A device’s start-up configuration
- A device’s current context configuration, such as profiles and policies

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show <PARAMETERS>

Parameters

- show <PARAMETERS>

The show command displays configuration details based on the configuration mode, in which the command is executed, and the parameters passed. For example, when executed in the AAA policy configuration mode, it displays the logged AAA policy’s current settings. The examples below show the configuration parameters that can be viewed in the User Executable, Priv Executable, and Global Configurable modes.

Examples

The following examples list the show commands in the User Exec, Priv Exec, and Global Config modes:

GLOBAL CONFIG Mode

<DEVICE>(config)#show ?
  adoption Display information related to adoption to
  bonjour wireless controller
  boot Bonjour Gateway related commands
  captive-portal Display boot configuration.
  captive-portal-page-upload Captive portal commands
  cdp Captive portal advanced page upload
  classify-url Cisco Discovery Protocol
  clock Query the category of an URL
  clock Display system clock
  cluster Cluster Protocol
  cmp-factory-certs Display the CMP certificate status
  commands Show command lists
  context Information about current context
  critical-resources Critical Resources
  crypto Encryption related commands
  database Database
  debug Debugging functions
  debugging Debugging functions
  device-upgrade Device Upgrade
  dot1x 802.1X
  dpi Deep Packet Inspection
  environmental-sensor Display Environmental Sensor Module status
  event-history Display event history
  event-system-policy Display event system policy
  ex3500 EX3500 device details
  extdev External device (T5, EX3500..)
  file Display filesystem information
  file-sync File sync between controller and adoptees
  firewall Wireless Firewall
SHOW COMMANDS 6-7

global                      Global-level information
gre                         Displays gre related information
guest-registration          Guest registration commands
interface                   Interface Configuration/Statistics commands
ip                          Internet Protocol (IP)
ip-access-list              IP ACL
ipv6                        Internet Protocol version 6 (IPv6)
ipv6-access-list            IPv6 ACL
l2tpv3                      L2TPV3 information
ldap-agent                  LDAP Agent Configuration
licenses                    Show installed licenses and usage
lldp                        Link Layer Discovery Protocol
logging                     Show logging information
mac-access-list             MAC ACL
mac-address-table           Display MAC address table
mac-auth                    MAC authentication
mac-auth-clients            MAC authenticated clients
mint                        MiNT protocol
mirroring                   Show mirroring sessions
ntp                         Network time protocol
password-encryption         Password encryption
pppoe-client                PPP Over Ethernet client
privilege                   Show current privilege level
radius                      RADIUS statistics commands
raid                        Show RAID status
reload                      Scheduled reload information
remote-debug                Show details of remote debug sessions
rf-domain-manager           Show RF Domain Manager selection details
role                        Role based firewall
route-maps                  Display Route Map Statistics
rtl5                        RTLS Statistics
running-config              Current operating configuration
session-changes             Configuration changes made in this session
session-config              This session configuration
sessions                    Display CLI sessions
site-config-diff            Difference between site configuration on the NOC
                            and actual site configuration
slot                        Expansion slots stats
smart-cache                 Content caching
smart-rf                    Smart-RF Management Commands
spanning-tree               Display spanning tree information
startup-config              Startup configuration
ts5                        TS5 details
terminal                    Display terminal configuration parameters
timezone                    The timezone
traffic-shape               Display traffic shaping
upgrade-status              Display last image upgrade status
version                     Display software & hardware version
virtual-machine             Virtual Machine
vrrp                        VRRP protocol
web-filter                  Web filter
what                        Perform global search
wireless                    Wireless commands
wwan                        Display wireless WAN Status

rfs7000-37FABE(config)#show clock
2015-06-06 13:05:41 UTC
rfs7000-37FABE(config)#
PRIVILEGE EXEC Mode

<DEVICE>#show ?

adoption Display information related to adoption to wireless controller
bonjour Bonjour Gateway related commands
boot Display boot configuration.
captive-portal Captive portal commands
captive-portal-page-upload Captive portal advanced page upload
cdp Cisco Discovery Protocol
classify-url Query the category of an URL
clock Display system clock
cluster Cluster Protocol
cmp-factory-certs Display the CMP certificate status
commands Show command lists
context Information about current context
critical-resources Critical Resources
crypto Encryption related commands
database Database
debug Debugging functions
devices Debugging functions
device-upgrade Device Upgrade
dot1x 802.1X
dpi Deep Packet Inspection
environmental-sensor Display Environmental Sensor Module status
event-history Display event history
event-system-policy Display event system policy
ex3500 EX3500 device details
extdev External device (T5, EX3500..)
file Display filesystem information
file-sync File sync between controller and adoptees
firewall Wireless Firewall
global Global-level information
gre Negate a command or set its defaults
guest-registration Guest registration commands
interface Interface Configuration/Statistics commands
ip Internet Protocol (IP)
ip-access-list IP ACL
ipv6 Internet Protocol version 6 (IPv6)
ipv6-access-list IPV6 ACL
l2tpv3 L2TPv3 information
ldap-agent LDAP Agent Configuration
licenses Show installed licenses and usage
lldp Link Layer Discovery Protocol
logging Show logging information
mac-access-list MAC ACL
mac-address-table Display MAC address table
mac-auth MAC authentication
mac-auth-clients MAC authenticated clients
mint MiNT protocol
mirroring Show mirroring sessions
ntp Network time protocol
password-encryption Password encryption
pppoe-client PPP Over Ethernet client
privilege Show current privilege level
radius RADIUS statistics commands
raid Show RAID status
reload Scheduled reload information
remote-debug Show details of remote debug sessions
rf-domain-manager Show RF Domain Manager selection details
role Role based firewall
route-maps Display Route Map Statistics
rtl5 RTL5 Statistics
running-config Current operating configuration
session-changes Configuration changes made in this session
session-config This session configuration
sessions Display CLI sessions
site-config-diff Difference between site configuration on the NOC and actual site configuration
slot Expansion slots stats
smart-cache Content caching
smart-rf                      Smart-RF Management Commands
spanning-tree                 Display spanning tree information
startup-config                Startup configuration
t5                            T5 details
terminal                      Display terminal configuration parameters
timezone                      The timezone
traffic-shape                 Display traffic shaping
upgrade-status                Display last image upgrade status
version                       Display software & hardware version
virtual-machine               Virtual Machine
vrrp                          VRRP protocol
web-filter                    Web filter
what                          Perform global search
wireless                      Wireless commands
wwan                          Display wireless WAN Status

<rfs7000-37FABE#>show terminal
Terminal Type: xterm
Length: 24     Width: 80
<rfs7000-37FABE#>

USER EXEC Mode
<rfs7000-37FABE#>show ?

adoption                      Display information related to adoption to wireless controller
bonjour                       Bonjour Gateway related commands
boot                          Display boot configuration.
captive-portal               Captive portal commands
captive-portal-page-upload   Captive portal advanced page upload
cdp                           Cisco Discovery Protocol
classify-url                 Query the category of an URL
clock                         Display system clock
cluster                       Cluster Protocol
cmp-factory-certs            Display the CMP certificate status
commands                     Show command lists
context                       Information about current context
critical-resources           Critical Resources
crypto                        Encryption related commands
database                      Database
debug                         Debugging functions
debugging                    Debugging functions
device-upgrade                Device Upgrade
dot1x                         802.1X
dpi                           Deep Packet Inspection
environmental-sensor         Display Environmental Sensor Module status
event-history                 Display event history
event-system-policy          Display event system policy
ex3500                        EX3500 device details
extdev                        External device (T5, EX3500..)
file                          Display filesystem information
file-sync                     File sync between controller and adoptees
firewall                      Wireless Firewall
global                       Global-level information
gre                           Negate a command or set its defaults
guest-registration            Guest registration commands
interface                    Interface Configuration/Statistics commands
ip                            Internet Protocol (IP))
ipv6                          Internet Protocol version 6 (IPv6)
licenses                     Show installed licenses and usage
lldp                          Link Layer Discovery Protocol
logging                      Show logging information
mac-address-table            Display MAC address table
mac-auth                      MAC authentication
mac-auth-clients              MAC authenticated clients
mint                          MiNT protocol
mirroring                     Show mirroring sessions
ntp                           Network time protocol
password-encryption           Password encryption
pppoe-client | PPP Over Ethernet client
privilege | Show current privilege level
radius | RADIUS statistics commands
rf-domain-manager | Show RF Domain Manager selection details
role | Role based firewall
route-maps | Display Route Map Statistics
rtls | RTLS Statistics
running-config | Current operating configuration
session-changes | Configuration changes made in this session
session-config | This session configuration
sessions | Display CLI sessions
site-config-diff | Difference between site configuration on the NOC and actual site configuration
slot | Expansion slots stats
smart-rf | Smart-RF Management Commands
spanning-tree | Display spanning tree information
startup-config | Startup configuration
t5 | T5 details
terminal | Display terminal configuration parameters
timezone | The timezone
traffic-shape | Display traffic shaping
version | Display software & hardware version
vrrp | VRRP protocol
web-filter | Web filter
what | Perform global search
wireless | Wireless commands
wwan | Display wireless WAN Status

<DEVICE>>

nx9500-6C8809(config)#show wireless ap configured

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap8132-74B45C</td>
<td>B4-C7-99-74-B4-5C</td>
<td>default-ap81xx</td>
<td>default</td>
<td>B4-C7-99-6D-B5-D4</td>
</tr>
<tr>
<td>2</td>
<td>ap6522-587258</td>
<td>B4-C7-99-58-72-58</td>
<td>default-ap6522</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</td>
<td>ap8132-711728</td>
<td>B4-C7-99-71-17-28</td>
<td>default-ap81xx</td>
<td>default</td>
<td>B4-C7-99-5C-FA-8E</td>
</tr>
<tr>
<td>4</td>
<td>rfs4000-880DA7</td>
<td>00-23-68-88-0D-A7</td>
<td>default-rfs4000</td>
<td>default</td>
<td>B4-C7-99-6C-88-09</td>
</tr>
<tr>
<td>5</td>
<td>ap7131-11E6C4</td>
<td>00-23-68-11-E6-C4</td>
<td>default-ap71xx</td>
<td>default</td>
<td>B4-C7-99-6D-B5-D4</td>
</tr>
<tr>
<td>6</td>
<td>rfs4000-229D58</td>
<td>00-23-68-22-9D-58</td>
<td>default-rfs4000</td>
<td>default</td>
<td>B4-C7-99-6C-88-09</td>
</tr>
</tbody>
</table>

nx9500-6C8809(config)#

The following Show commands are specific to the NX45XX and NX65XX series service platforms:

nx4500-5CFA2B>show slot

<table>
<thead>
<tr>
<th>SLOT</th>
<th>TYPE</th>
<th>MODULE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[]</td>
<td>wing</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>[]</td>
<td>wing</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>[]</td>
<td>wing</td>
<td>Enabled</td>
</tr>
<tr>
<td>4</td>
<td>[]</td>
<td>wing</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B>

nx4500-5CFA2B#show smart-cache ?

active-requests | Active requests
clients | Client list
purge-requests | Purge-requests
statistics | Statistics
storage | Storage

nx4500-5CFA2B#
nx4500-5CFA2B# show smart-cache storage

---

<table>
<thead>
<tr>
<th>USED</th>
<th>TOTAL</th>
<th>USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1592</td>
<td>33554432</td>
<td>0%</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B#

nx4500-5CFA2B(config)# show smart-cache statistics

---

<table>
<thead>
<tr>
<th>DURATION</th>
<th>DATA (KB)</th>
<th>BANDWIDTH (Kbps)</th>
<th>REQUESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TOTAL CACHE</td>
<td>WAN CACHE</td>
<td>TOTAL CACHE</td>
</tr>
<tr>
<td>Since boot</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B(config)#

nx4500-5CFA2B(config)# show virtual-machine statistics

---

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATE</th>
<th>VCPUS</th>
<th>MEM (MB)</th>
<th>BRIDGE-IF</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>team-rls</td>
<td>(not_installed)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>team-urc</td>
<td>Running</td>
<td>1</td>
<td>1200</td>
<td>eth0 (vmif2)</td>
<td>192.168.13.103</td>
</tr>
<tr>
<td>team-vowlan</td>
<td>(not_installed)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B(config)#

The following Show commands are specific to the NX9500 series service platform:

nx9500-6C874D> show raid
Logical drive info:
Size 930 GB, State optimal
Alarm enabled
Last check: Tue Jun 2 20:37:20 2015
Last check result: done

Physical drive info:
Drive slot 0: online
Drive slot 1: online
Drive slot 2: not-installed
Drive slot 3: not-installed
Drive slot 4: not-installed

nx9500-6C874D>

The following show commands are specific to the NX9500 and NX9510 series service platforms:

nx9500-6C874D(config)# show virtual-machine configuration

---

<table>
<thead>
<tr>
<th>NAME</th>
<th>AUTOSTART</th>
<th>MEMORY (MB)</th>
<th>VCPUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WING</td>
<td>-</td>
<td>16384</td>
<td>-</td>
</tr>
<tr>
<td>adsp</td>
<td>start</td>
<td>16384</td>
<td>12</td>
</tr>
<tr>
<td>team-cmt</td>
<td>start</td>
<td>1024</td>
<td>1</td>
</tr>
</tbody>
</table>

nx9500-6C874D(config)#
### 6.1.2 adoption

#### show commands

Displays adoption related information, and is common to the User Exec, Priv Exec, and Global Config modes.

In an hierarchically managed (HM) network devices are deployed in two levels. The first level consists of the Network Operations Center (NOC) controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (access points and second-level controllers) are referred to as the adoptee. The devices adopting the adoptee are the ‘adopters’.

Use this command to confirm if a device is an adoptee or an adopter. This command also allows you to determine the devices adopted by an adopter device.

**NOTE:** A NOC controller’s capacity is equal to or higher than a site controller’s capacity. The following devices can be deployed at NOC and sites:

- NOC controller – RFS6000, RFS7000, NX65XX, NX9000, NX9500, NX9510, or NX9600.
- Site controller – NX45XX, NX65XX, RFS7000, RFS6000, or RFS4000.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show adoption [config-errors|controllers|history|info|log|offline|pending|status|timeline]`

`show adoption offline`

`show adoption config-errors <DEVICE-NAME>`

`show adoption log [adoptee|adopter {<MAC>}] {on <DEVICE-NAME>}`

`show adoption [controllers|history|info|pending|status|timeline] {on <DEVICE-NAME>}`

**Parameters**

- show adoption offline

| adoption | Displays adoption related information. It also displays configuration errors. |
| offline | Displays non-adopted status of the logged device and its adopted access points |

- show adoption config-errors <DEVICE-NAME>

| adoption | Displays adoption related information. It also displays configuration errors. |
| config-errors <DEVICE-NAME> | Displays configuration errors for a specified adopted device
- `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |

- show adoption log [adoptee|adopter {<MAC>}] {on <DEVICE-NAME>}

| adoption | Displays adoption related information. It also displays configuration errors. |
show adoption history [history|controllers|info|pending|status|timeline] {on <DEVICE-NAME>}

- **adoption**
  Displays adoption related information. It also displays configuration errors.

- **controllers**
  Displays information about adopted controllers. This is applicable in a Hierarchically managed network, where site controllers are adopted by the NOC controllers.

- **history**
  Displays adoption history of the logged device and its adopted access points

- **info**
  Displays adopted device information

- **pending**
  Displays information for devices pending adoption

- **status**
  Displays adoption status for logged devices

- **timeline**
  Displays the logged device’s adoption timeline. It also shows the adoption time for logged device’s adopted APs. To view the adoption timeline of a specific device, use the on <device-name> option to specify the device.

- **on <DEVICE-NAME>**
  The following keywords are common to all of the above parameters:
  - on <DEVICE-NAME> – Optional. Displays a device’s adoption information, based on the parameter passed.
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

- **log [adoptee|adopter {MAC}] {on <DEVICE-NAME>}
  Displays adoption logs, for the specified device. If no device name is specified, the system displays logs for the logged device.
  
  - adoptee – Displays adoption logs for adoptee devices (APs, wireless controllers, and service platforms). To view logs for a specified adoptee, specify the device’s name. If no device name is specified, the system displays logs for the logged device. If the logged device is not an adoptee, the system states that the device is a controller.
    For example, 2013-01-19 22:00:13:MLCP_TAG_CLUST Master not present and this device is a controller. Ignoring
  
  - on <DEVICE-NAME> – Optional. Displays adoptee status and details for the device identified by the <DEVICE-NAME> keyword
    - <DEVICE-NAME> – Specify the device’s name.
  
  - adopter – Displays adoption logs for adopter devices (APs, wireless controllers, and service platforms). To view logs for a specified adopter, specify the device’s name. If no device name is specified, the system displays logs for the logged device.
    - <MAC> – Optional. Filters adopters by the adopted device’s MAC address. Specify the adopted device’s MAC address. The system displays logs for the device that has adopted the device identified by the <MAC> keyword.
    - on <DEVICE-NAME> – Optional. Displays adopter status and details for the device identified by the <DEVICE-NAME> keyword.
    - <DEVICE-NAME> – Specify the adopter device’s name.

- **Note:** A wireless controller or service platform cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted wireless controller or service platform cannot be configured to adopt another device and vice versa.
Usage Guidelines

In a device's Global Config mode, use the `customize > show-adoption-status` command to customize the `show > adoption > status` command output. The following columns can be added to the output:

```
adopted-by     Device name to which the AP is adopted
ap-name        Host-name of the adopted AP
cdp-lldp-info  Cdp/lldp info of the Adopted AP
config-status  Configuration status of the adopted AP
last-adoption  Last known adoption time
msgs           Messages status
uptime         Uptime of the adopted AP
version        Current version of the adopted AP
```

For more information on the `customize` command, see `customize`.

Examples

The following example displays details of the:

- logged device (`rfs6000-81742D`), and
- devices adopted (`ap8132-711728`) by the logged device.

```
rfs6000-81742D#show adoption status
Adopted by:
Type          : RFS7000
System Name   : rfs7000-6DCD4B
MAC address   : B4-C7-99-6D-CD-4B
MiNT address  : 19.6D.CD.4B
Time          :   0 days 00:18:43 ago
Adopted Devices:
------------------------------------------------------------------------
ADOPTED-BY        DEVICE-NAME       CFG-STAT       LAST-ADOPTION
------------------------------------------------------------------------
rfs6000-81742D  ap8132-711728     configured  0 days 00:05:20
------------------------------------------------------------------------
Total number of devices displayed: 1
```

```
rfs6000-81742D#show adoption offline
------------------------------------------------------------------------
MAC            HOST-NAME      TYPE     RF-DOMAIN  TIME OFFLINE   CONNECTED-TO
------------------------------------------------------------------------
11-22-33-44-55-66    t5-445566       t5      default      unknown        None
B4-C7-99-58-72-58  ap6522-587258   ap6522    default        unknown        None
B4-C7-99-71-17-28  ap8132-711728   ap81xx    default        unknown        None
B4-C7-99-74-B4-5C  ap8132-74B45C   ap81xx    default        unknown        None
------------------------------------------------------------------------
Total number of devices displayed: 4
```

```
ap7131-11E6C4(config)#show adoption log adoptee
2015-06-01 08:56:55:Received OK from cfgd, adoption complete to 19.5C.FA.2B
2015-06-01 08:56:54:Waiting for cfgd OK, adopter should be 19.5C.FA.2B
2015-06-01 08:56:54:Try to adopt to 19.5C.FA.2B (cluster master 19.5C.FA.2B in adopters)
2015-06-01 08:56:24:Ignoring MLCP Offer, vlan_state MLCP_DONE != MLCP_DISCOVERING / MLCP_STP_WAITING
2015-06-01 08:56:24:MLCP created VLAN link on VLAN 1, offer from B4-C7-99-5C-FA-2B
2015-06-01 08:56:24:MLCP VLAN link already exists
2015-06-01 08:56:24:Ignoring MLCP Offer, vlan_state MLCP_REPLY_WAIT != MLCP_DISCOVERING / MLCP_STP_WAITING
--More--
ap7131-11E6C4(config)#
```
nx9500-6C8809#show adoption controllers

<table>
<thead>
<tr>
<th>NAME</th>
<th>RF-DOMAIN</th>
<th>MAC</th>
<th>MINT-ID</th>
<th>IP</th>
<th>ADOPTED-BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs6000-380649</td>
<td>default</td>
<td>00-15-70-38-06-49 70.38.06.49</td>
<td>192.168.13.6</td>
<td>nx9500-6C8809</td>
<td></td>
</tr>
<tr>
<td>nx4500-5CFA8E</td>
<td>default</td>
<td>B4-C7-99-5C-FA-8E 19.5C.FA.8E</td>
<td>192.168.0.1</td>
<td>nx9500-6C8809</td>
<td></td>
</tr>
<tr>
<td>rfs6000-6DB5D4</td>
<td>default</td>
<td>B4-C7-99-6D-B5-D4 19.6D.B5.D4</td>
<td>192.168.13.16</td>
<td>nx9500-6C8809</td>
<td></td>
</tr>
</tbody>
</table>

Total number of devices displayed: 4

nx9500-6C8809(config)#show adoption history

<table>
<thead>
<tr>
<th>MAC</th>
<th>TYPE</th>
<th>EVENT</th>
<th>TIME-STAMP</th>
<th>REASON</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6D-B5-D4</td>
<td>RFS6000</td>
<td>adopted</td>
<td>2015-06-01 08:58:03</td>
<td>N.A.</td>
</tr>
<tr>
<td>B4-C7-99-5C-FA-8E</td>
<td>NX45XX</td>
<td>adopted</td>
<td>2015-06-01 08:56:50</td>
<td>N.A.</td>
</tr>
<tr>
<td>00-15-70-38-06-49</td>
<td>RFS6000</td>
<td>adopted</td>
<td>2015-06-01 08:56:46</td>
<td>N.A.</td>
</tr>
<tr>
<td>B4-C7-99-5C-FA-2B</td>
<td>NX45XX</td>
<td>adopted</td>
<td>2015-06-01 08:56:29</td>
<td>N.A.</td>
</tr>
</tbody>
</table>

nx9500-6C8809(config)#
6.1.3 boot

*show commands*

Displays a device’s boot configuration. Use this command to view the primary and secondary image details, such as Build Date, Install Date, and Version. This command also displays the current boot and next boot information.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show boot {on <DEVICE-NAME>}
```

**Parameters**

- **on** `<DEVICE-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>Displays primary and secondary image boot configuration details (build date, install date, version, and the image used to boot the current session)</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Displays a specified device’s boot configuration</td>
</tr>
</tbody>
</table>

- `<DEVICE-NAME>` — Specify the name of the AP, wireless controller, or service platform.

**Note:** Use the `on `<DEVICE-NAME>` option to view a remote device’s boot configuration.

**Examples**

```
rfs4000-229D58(config)#show boot
------------------------------------------------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>IMAGE</th>
<th>BUILD DATE</th>
<th>INSTALL DATE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>05/31/2015 00:05:49</td>
<td>06/01/2015 08:53:42</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>Secondary</td>
<td>05/23/2015 19:05:24</td>
<td>05/26/2015 08:25:26</td>
<td>5.8.1.0-034B</td>
</tr>
</tbody>
</table>
------------------------------------------------------------------------------------------------------------------------------------
Current Boot : Primary
Next Boot : Primary
Software Fallback : Enabled
rfs4000-229D58(config)#
```
6.1.4 bonjour

show commands

Displays the configured Bonjour services available on local and remote sites

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show bonjour services {on <DEVICE-NAME>}

Parameters

- show bonjour services {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>bonjour services</th>
<th>Displays the configured Bonjour services available on local and remote sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays Bonjour services available on a specified device</td>
</tr>
<tr>
<td></td>
<td>&lt;DEVICE-NAME&gt; — Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE#show bonjour services on ap7131-11E6C4

------------------------------------------
<table>
<thead>
<tr>
<th>SERVICE_NAME</th>
<th>INSTANCE_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>_home-sharing._tcp.local</td>
<td>bob’s</td>
</tr>
<tr>
<td>Library_05ADD1A42FA8_1._home-sharing._tcp.local</td>
<td>41.41.112.3689 41 Local Fri Feb 28 02:26:24 2014</td>
</tr>
<tr>
<td>_00000000-77ed-3b41-c561-f8238e524864._sub._home-sharing._tcp.local</td>
<td>bob’s</td>
</tr>
<tr>
<td>Library_05ADD1A42FA8_1._home-sharing._tcp.local</td>
<td>41.41.112.3689 41 Local Fri Feb 28 02:26:24 2014</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#
### 6.1.5 captive-portal

#### show captive-portal

Displays WLAN captive portal information. Use this command to view a configured captive portal's client information.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
show captive-portal sessions {include-ipv6|on <DEVICE-OR-DOMAIN-NAME>|statistics}
```

#### Parameters

- **captive-portal sessions**
  - Displays active captive portal client session details
- **include-ipv6**
  - Optional. Includes IPv6 address (if known) of captive portal clients
  - **Note:** By default the system only displays IPv4 addresses. The include-ipv6 parameter includes IPv6 address (if known) of each client.
- **statistics**
  - Optional. Displays statistical information regarding client sessions
- **on <DEVICE-OR-DOMAIN-NAME>**
  - Optional. Displays active captive portal session details on a specified device or RF Domain.
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.
- **filter**
  - This parameter is recursive and can be used with any of the above parameters to define additional filters.
  - Optional. Defines additional filters. Use one of the following options: captive-portal, ip, ipv6, state, vlan, or wlan.
- **captive-portal [<CAPTIVE-PORTAL>|not <CAPTIVE-PORTAL>]**
  - Optional. Displays captive portal client and client session information, based on the captive portal name passed
  - `<CAPTIVE-PORTAL>` – Specify the captive portal name. Displays client details for the specified captive portal.
  - not `<CAPTIVE-PORTAL>` – Inverts the match selection. Displays client details for all captive portals other than the specified captive portal.
- **ip [<IPv4>|not <IPv4>]**
  - Optional. Displays captive portal client/client sessions information, based on the IPv4 address passed
  - `<IPv4>` – Specify the client's IPv4 address. Displays information of the client identified by the `<IPv4>` parameter
  - not `<IPv4>` – Inverts the match selection. Displays client details for all clients other than the one identified by the `<IPv4>` parameter.
### Examples

```
rfs4000-229D58#show captive-portal sessions
=======================================================================================
CLIENT               IPv4     CAPTIVE-PORTAL   WLAN/PORT    VLAN  STATE SESSION  TIME
---------------------------------------------------------------------------------------
00-26-55-F4-5F-79  192.168.3.99 cappo     rfs4000-229D58:ge2    400     Success     23:58:35
=======================================================================================
Total number of captive portal sessions displayed: 1
rfs4000-229D58#
```
### 6.1.6 captive-portal-page-upload

**show commands**

Displays captive portal page information, such as upload history, upload status, and page file download status

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show captive-portal-page-upload [history|load-image-status|status]
show captive-portal-page-upload load-image-status
show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}
show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]} 
```

**Parameters**

- `show captive-portal-page-upload load-image-status`
- `show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}
- `show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}`  

**Examples**

```
rfs7000-37FABE>show captive-portal-page-upload status
Number of APs currently being uploaded : 0
Number of APs waiting in queue to be uploaded : 0

--------------------------------------------------------------------------------
AP STATE UPLOAD TIME PROGRESS RETRIES LAST UPLOAD ERROR    UPLOADED BY
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
rfs7000-37FABE>
```
```
rfs7000-37FABE>show captive-portal-page-upload history
---------------------------------------------------------------------------------------
AP RESULT TIME RETRIES Uploaded-By LAST-UPLOAD-ERROR
---------------------------------------------------------------------------------------
No upload history is present
rfs7000-37FABE>
```
```
rfs7000-37FABE>show captive-portal-page-upload load-image-status
No captive portal advanced page file download is in progress
rfs7000-37FABE>
```
### 6.1.7 cdp

- **show commands**

  Displays the *Cisco Discovery Protocol* (CDP) neighbor table

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

  **Syntax**

  ```
  show cdp [neighbors/report] {detail {on <DEVICE-NAME>}}|on <DEVICE-NAME>
  ```

  **Parameters**

  - `show cdp [neighbors/report] {detail {on <DEVICE-NAME>}}|on <DEVICE-NAME>`

  - **cdp [neighbors/report]** Displays CDP neighbors table or aggregated CDP neighbors table
  - **detail {on <DEVICE-NAME>**} Optional. Displays detailed CDP neighbors table or aggregated CDP neighbors table
  - **on <DEVICE-NAME>** Optional. Displays table details on a specified device

  - `<DEVICE-NAME>` Specify the name of the AP, wireless controller, or service platform.

  **Examples**

  The following example shows detailed CDP neighbors table:

  ```
  nx4500-5CFA2B#show cdp neighbors detail
  -------------------------
  Device ID: rfs4000-880DA7
  Entry address(es):
    IP Address: 192.168.13.8
    IP Address: 192.168.0.1
    IP Address: 1.2.3.4
  Platform: RFS-4011-11110-US, Capabilities: Router Switch
  Interface: up1, Port ID (outgoing port): ge1
  Hold Time: 154 sec
  -------------------------
  Device ID: ap5142-587258
  Entry address(es):
  IP Address: 192.168.13.24
  Platform: AP-5142-66040-WR, Capabilities: Router
  Interface: up1, Port ID (outgoing port): ge1
  Hold Time: 178 sec
  --More--
  nx4500-5CFA2B#
  ```
The following example shows a non-detailed CDP neighbors table:

```
nx4500-5CFA2B#show cdp neighbors
+-------------------------------+-----------------+-------------------+----------+-------+
| Device ID                     | Platform        | Local Interface   | Port ID  | Duplex|
+-------------------------------+-----------------+-------------------+----------+-------+
| rfs7000-6DCD4B                | RFS-7010-1000-WR| up1               | ge2      | full  |
| rfs6000-6DB5D4                | RFS-6010-1000-WR| up1               | ge1      | full  |
| rfs7000-181091                | RFS-7010-1000-WR| up1               | ge1      | full  |
| nx9500-6C8809                 | NX-9500-100R0-WR| up1               | ge1      | full  |
+-------------------------------+-----------------+-------------------+----------+-------+

rfs7000-6DCD4B>show cdp neighbors
+-------------------------------+-----------------+-------------------+----------+-------+
| Device ID                     | Platform        | Local Interface   | Port ID  | Duplex|
+-------------------------------+-----------------+-------------------+----------+-------+
| ap8132-74B45C                 | AP-8132-66040-WR| ge2               | ge1      | full  |
| CiscoLab                      | cisco WS-C2960S-24PS-L| ge2          | GigabitEthernet1/0/3 | full |
| nx4500-5CFA8E                 | NX-4500-0000-00-WR| ge2               | up1      | full  |
| L3-Router                     | RFS-4010-00010-WR| ge1               | ge2      | full  |
| nx4500-5CFA2B                 | NX-4500-0000-00-WR| ge2               | up1      | full  |
+-------------------------------+-----------------+-------------------+----------+-------+
```

rfs7000-6DCD4B>
6.1.8 classify-url

Displays a specified URL's category. Use this command to query the category of a specific URL. The query is sent to a configured classification server. This option is available only if a valid URL filter license is available.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show classify-url [<URL-TO-QUERY>|datacenter <URL-TO-QUERY>]
```

**Parameters**

- `show classify-url [<URL-TO-QUERY>|datacenter <URL-TO-QUERY>]`

<table>
<thead>
<tr>
<th>classify-url</th>
<th>Queries the category of a specified URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;URL-TO-QUERY&gt;</td>
<td>Specify the URL to query. The query is sent to the configured classification server.</td>
</tr>
<tr>
<td>datacenter</td>
<td>The query is sent to a global classification datacenter</td>
</tr>
<tr>
<td>&lt;URL-TO-QUERY&gt;</td>
<td>• &lt;URL-TO-QUERY&gt; – Specify the URL to query.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx4500-5CFA2B# show classify-url www.google.com
Categories: search-engines-portals,
Custom Categories:
nx4500-5CFA2B#
```

```
nx4500-5CFA2B# show classify-url www.ndtv.com
Categories: news,
Custom Categories: list1,
nx4500-5CFA2B#
```
### 6.1.9 clock

*show commands*

Displays a selected system’s clock

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show clock {on <DEVICE-NAME>}
```

**Parameters**

- `show clock {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>Displays a system’s clock</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays system clock on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#show clock
2015-06-05 05:48:46 UTC
rfs7000-37FABE(config)#
```
6.1.10 cluster

> show commands

Displays cluster information (cluster configuration parameters, members, status etc.)

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show cluster [configuration|members|status]
show cluster [configuration|members {detail}|status]
```

**Parameters**

- `show cluster [configuration|members {detail}|status]`

<table>
<thead>
<tr>
<th>cluster</th>
<th>Displays cluster information</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Displays cluster configuration parameters</td>
</tr>
<tr>
<td>members {detail}</td>
<td>Displays cluster members configured on the logged device</td>
</tr>
<tr>
<td>status</td>
<td>Displays cluster status</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#show cluster configuration

    Name                               : TechPubsLan
    Configured Mode                    : Active
    Master Priority                    : 128
    Force configured state             : Disabled
    Force configured state delay       : 5 minutes
    Handle STP                         : Disabled
    Radius Counter DB Sync Time        : 5 minutes
```

```
rfs7000-37FABE(config)#show cluster members detail

<table>
<thead>
<tr>
<th>ID</th>
<th>MAC</th>
<th>MODE</th>
<th>AP COUNT</th>
<th>AAP COUNT</th>
<th>AP LICENSE</th>
<th>AAP LICENSE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.6D.CD.4B</td>
<td>B4-C7-99-6D-CD-4B</td>
<td>Active</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5.8.1.0-034B</td>
</tr>
</tbody>
</table>
```

```
rfs7000-37FABE(config)#show cluster status

    Cluster Runtime Information
    Protocol version    : 1
    Cluster operational state : active
    AP license          : 0
    AAP license         : 0
    AP count            : 0
    AAP count           : 0
    Max AP adoption capacity : 1024
    Number of connected member(s) : 0
```

rfs7000-37FABE(config)#
6.1.11 **cmp-factory-certs**

Displays factory installed CMP certificates

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show cmp-factory-certs {all}
```

**Parameters**

- `show cmp-factory-certs {all}`

**Examples**

```
nx9500-6C8809>show cmp-factory-certs
No CMP factory certificate exist
nx9500-6C8809>
```
### 6.1.12 commands

**show commands**

Displays commands available for the current mode

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show commands`

**Parameters**

None

**Examples**

```bash
rfs4000-229D58(config)#show commands
help
help search WORD (|detailed|only-show|skip-show|skip-no)
show commands
show adoption log adoptee(|(on DEVICE-NAME))
show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|(on DEVICE-NAME))
show adoption info (|(on DEVICE-NAME))
show adoption status (|(on DEVICE-NAME))
show adoption config-errors DEVICE-NAME
show adoption offline
show adoption pending (|(on DEVICE-NAME))
show adoption history (|(on DEVICE-NAME))
show debugging ([|on DEVICE-OR-DOMAIN-NAME])
show debugging cfdg
show debugging fib(|(on DEVICE-NAME))
show debugging adoption ([|on DEVICE-OR-DOMAIN-NAME])
show debugging wireless ([|on DEVICE-OR-DOMAIN-NAME])
show debugging snmp (|(on DEVICE-NAME))
show debugging ssn (|(on DEVICE-NAME))
show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))
show debugging captive-portal (|(on DEVICE-OR-DOMAIN-NAME))
show debugging dhcpsvr (|(on DEVICE-NAME))
show debugging role (|(on DEVICE-OR-DOMAIN-NAME))
show debugging dot1x(|(on DEVICE-NAME))
--More--
rfs4000-229D58(config)#
```

```bash
nx4500-5CFA2B(config)#show commands
help
help search WORD (|detailed|only-show|skip-show|skip-no)
show commands
show adoption log adoptee(|(on DEVICE-NAME))
show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|(on DEVICE-NAME))
show adoption info (|(on DEVICE-NAME))
show adoption status (|(on DEVICE-NAME))
show adoption config-errors DEVICE-NAME
show adoption offline
show adoption pending (|(on DEVICE-NAME))
show adoption history (|(on DEVICE-NAME))
show debugging ([|on DEVICE-OR-DOMAIN-NAME])
show debugging cfdg
```

--More--

```bash
nx4500-5CFA2B(config)#
```
6.1.13 context

- show commands
  Displays the current context details

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show context {include-factory|session-config {include-factory}}

Parameters
- show context {include-factory|session-config {include-factory}}

<table>
<thead>
<tr>
<th>include-factory</th>
<th>Optional. Includes factory defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-config</td>
<td>Optional. Displays running system information in the current context</td>
</tr>
<tr>
<td>{include-factory}</td>
<td>• include-factory – Optional. Includes factory defaults</td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.8.1.0-035B
!
!
version 2.3
!
client-identity Android-2-2
dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
client-identity Android-2-3
dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
dhcp 6 message-type request option 60 exact ascii "dhcpcd 4.0.15"
dhcp 1 message-type request option-codes exact hexstring 353d32393c37
dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
!
client-identity Android-2-3-x
dhcp 10 message-type request option 55 exact hexstring 01792103060f1c333a3b77
dhcp 11 message-type request option 55 exact hexstring 01792103060f1c2c333a3b77
dhcp 12 message-type request option 60 exact ascii "dhcpcd 4.0.15"
!
--More--
rfs4000-229D58(config)#
### 6.1.14 critical-resources

*show commands*

Displays critical resource information. Critical resources are resources vital to the network.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```bash
show critical-resources {on <DEVICE-NAME>}
```

**Parameters**

- `show critical-resources {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>critical-resources</th>
<th>Displays critical resources information</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays critical resource information on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs4000-229D58(config)#show critical-resources
-------------------------------------------------------------------------
CRITICAL RESOURCE IP        VLAN          PING-MODE            STATE
-------------------------------------------------------------------------
172.168.1.103                1             arp-icmp             up
-------------------------------------------------------------------------

rfs4000-229D58(config)#
```
6.1.15 crypto

> show commands

Displays encryption mode information

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
show crypto [cmp|ike|ipsec|key|pki]
```

```
show crypto cmp request status
```

```
show crypto ike sa {detail|on|peer <IP>} {on <DEVICE-NAME>}
```

```
show crypto ike sa {version [1|2]} {peer <IP>} {on <DEVICE-NAME>}
```

```
show crypto ipsec sa {detail|on|peer}
```

```
show crypto ipsec sa {detail} {on <DEVICE-NAME>}
```

```
show crypto key rsa {on|public-key-detail}
```

```
show crypto key rsa {public-key-detail} {on <DEVICE-NAME>}
```

```
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all|on}
```

```
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}
```

Parameters

- **show crypto cmp request status**

  Displays current status of in-progress certificate management protocol (CMP) requests

  **Note:** For more information, see Chapter 29, CRYPTO-CMP-POLICY.

- **show crypto ike sa {detail|on|peer <IP>} {on <DEVICE-NAME>}

  Displays Internet Key Exchange (IKE) security association (SA) statistics

  **peer <IP>**

  Optional. Displays IKE SA statistics for a specified peer

  - <IP> – Specify the peer’s IP address in the A.B.C.D format

  **on <DEVICE-NAME>**

  Optional. Displays IKE SA statistics on a specified device

  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

- **show crypto ike sa {version [1|2]} {peer <IP>} {on <DEVICE-NAME>}

  Displays IKE SA details

  **version [1|2]**

  Optional. Displays IKE SA version statistics

  - 1 – Displays IKEv1 statistics
  - 2 – Displays IKEv2 statistics
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer &lt;IP&gt;</code></td>
<td>Optional. Displays IKE SA version statistics for a specified peer</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP&gt;</code> – Specify the peer’s IP address in the A.B.C.D format</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keyword is recursive and common to the ‘peer ip’ parameter:</td>
</tr>
<tr>
<td></td>
<td>• <code>on &lt;DEVICE-NAME&gt;</code> – Optional. Displays IKE SA statistics on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td></td>
<td>• <code>show crypto ipsec sa {detail} {on &lt;DEVICE-NAME&gt;}</code></td>
</tr>
<tr>
<td><code>crypto ipsec sa</code></td>
<td>Displays Internet Protocol Security (IPSec) SA statistics. The IPSec encryption</td>
</tr>
<tr>
<td></td>
<td>authenticates and encrypts each IP packet in a communication session</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>Optional. Displays detailed IPSec SA statistics</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Displays IPSec SAs on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><code>peer &lt;IP&gt; detail</code></td>
<td>Optional. Displays IPSec SA statistics for a specified peer</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP&gt;</code> – Specify the peer’s IP address in the A.B.C.D format</td>
</tr>
<tr>
<td></td>
<td>• <code>detail</code> – Displays detailed IPSec SA statistics for the specified peer</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keyword is recursive:</td>
</tr>
<tr>
<td></td>
<td>• <code>on &lt;DEVICE-NAME&gt;</code> – Optional. Displays IPSec SAs on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><code>crypto key rsa</code></td>
<td>Displays RSA public keys</td>
</tr>
<tr>
<td></td>
<td><code>public-key-detail</code> Optional. Displays public key in the Privacy-Enhanced Mail (PEM) format</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keyword is recursive:</td>
</tr>
<tr>
<td></td>
<td>• <code>on &lt;DEVICE-NAME&gt;</code> – Optional. Displays public key on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><code>crypto pki trustpoints</code></td>
<td>Displays WLAN trustpoints</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Optional. Displays a specified trustpoint details. Specify the trustpoint name.</td>
</tr>
<tr>
<td></td>
<td><code>all</code> Optional. This command displays all trustpoints including CMP-generated trustpoints.</td>
</tr>
</tbody>
</table>
Examples

```
nx9500-6C8809#show crypto key rsa public-key-detail
RSA key name: ting Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj11yR38+/mcInGR1rw
3DaasuTuHksw7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TuM
Z4YgKtz1ANSAG7EZRBr3MXEIH49NHYeK8U+1EAmHN9F21XCxTO+yRNgkDJeHfz
Za2/64PDbnRLv4nqCGM0HbbaaCwGe5X0a
-----END PUBLIC KEY-----

RSA key name: default_rsa_key Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAdyJDk9aMk97X3PhoyMb
6nuFLFUKpFP9YwSq2fNy9p8tqopML/VAMhHotmaa56xPURF8mC6bT7De32r7
wwPd7p1WwALTscwCzd1Crbjy8a2OQ7ZHGC6MLau+LeoNPE0c+uH3tNLloTAvSG
xtUAHfwFa4rM6vLzs/ejJ4ImboI8i4uIA
-----END PUBLIC KEY-----
```

```
nx9500-6C8809#show crypto key rsa
#            KEY NAME         KEY LENGTH
#          #               KEY LENGTH
1          ting                   2048
2          default_rsa_key       2048
```

```
nx9500-6C8809#show crypto pkp trustpoints all
Trustpoint Name: default-trustpoint (self signed)
CRL present: no
Server Certificate details:
  Key used: default_rsa_key
  Serial Number: 051d
  Subject Name: /CN=NX9500-B4-C7-99-6C-88-09
  Issuer Name: /CN=NX9500-B4-C7-99-6C-88-09
  Valid From: Thu Dec  5 04:15:59 2013 UTC
  Valid Until: Sun Dec  3 04:15:59 2023 UTC
```

```
nx9500-6C8809>show crypto cmp request status
CMP Request Status: ir-req-reset
```

```
nx9500-6C8809>show crypto key rsa public-key-detail
RSA key name: ting Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj11yR38+/mcInGR1rw
3DaasuTuHksw7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TuM
Z4YgKtz1ANSAG7EZRBr3MXEIH49NHYeK8U+1EAmHN9F21XCxTO+yRNgkDJeHfz
Za2/64PDbnRLv4nqCGM0HbbaaCwGe5X0a
-----END PUBLIC KEY-----

RSA key name: default_rsa_key Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAdyJDk9aMk97X3PhoyMb
6nuFLFUKpFP9YwSq2fNy9p8tqopML/VAMhHotmaa56xPURF8mC6bT7De32r7
wwPd7p1WwALTscwCzd1Crbjy8a2OQ7ZHGC6MLau+LeoNPE0c+uH3tNLloTAvSG
xtUAHfwFa4rM6vLzs/ejJ4ImboI8i4uIA
-----END PUBLIC KEY-----
```

```
nx9500-6C8809#show crypto key rsa
#            KEY NAME         KEY LENGTH
#          #               KEY LENGTH
1          ting                   2048
2          default_rsa_key       2048
```

```
nx9500-6C8809#show crypto pkp trustpoints all
Trustpoint Name: default-trustpoint (self signed)
CRL present: no
Server Certificate details:
  Key used: default_rsa_key
  Serial Number: 051d
  Subject Name: /CN=NX9500-B4-C7-99-6C-88-09
  Issuer Name: /CN=NX9500-B4-C7-99-6C-88-09
  Valid From: Thu Dec  5 04:15:59 2013 UTC
  Valid Until: Sun Dec  3 04:15:59 2023 UTC
```

```
nx9500-6C8809>show crypto cmp request status
CMP Request Status: ir-req-reset
```

```
nx9500-6C8809>show crypto key rsa public-key-detail
RSA key name: ting Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj11yR38+/mcInGR1rw
3DaasuTuHksw7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TuM
Z4YgKtz1ANSAG7EZRBr3MXEIH49NHYeK8U+1EAmHN9F21XCxTO+yRNgkDJeHfz
Za2/64PDbnRLv4nqCGM0HbbaaCwGe5X0a
-----END PUBLIC KEY-----

RSA key name: default_rsa_key Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAdyJDk9aMk97X3PhoyMb
6nuFLFUKpFP9YwSq2fNy9p8tqopML/VAMhHotmaa56xPURF8mC6bT7De32r7
wwPd7p1WwALTscwCzd1Crbjy8a2OQ7ZHGC6MLau+LeoNPE0c+uH3tNLloTAvSG
xtUAHfwFa4rM6vLzs/ejJ4ImboI8i4uIA
-----END PUBLIC KEY-----
```

```
nx9500-6C8809#show crypto key rsa
#            KEY NAME         KEY LENGTH
#          #               KEY LENGTH
1          ting                   2048
2          default_rsa_key       2048
```

```
nx9500-6C8809#show crypto pkp trustpoints all
Trustpoint Name: default-trustpoint (self signed)
CRL present: no
Server Certificate details:
  Key used: default_rsa_key
  Serial Number: 051d
  Subject Name: /CN=NX9500-B4-C7-99-6C-88-09
  Issuer Name: /CN=NX9500-B4-C7-99-6C-88-09
  Valid From: Thu Dec  5 04:15:59 2013 UTC
  Valid Until: Sun Dec  3 04:15:59 2023 UTC
```

```
nx9500-6C8809>show crypto cmp request status
CMP Request Status: ir-req-reset
```

```
nx9500-6C8809>show crypto key rsa public-key-detail
RSA key name: ting Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj11yR38+/mcInGR1rw
3DaasuTuHksw7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TuM
Z4YgKtz1ANSAG7EZRBr3MXEIH49NHYeK8U+1EAmHN9F21XCxTO+yRNgkDJeHfz
Za2/64PDbnRLv4nqCGM0HbbaaCwGe5X0a
-----END PUBLIC KEY-----

RSA key name: default_rsa_key Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAdyJDk9aMk97X3PhoyMb
6nuFLFUKpFP9YwSq2fNy9p8tqopML/VAMhHotmaa56xPURF8mC6bT7De32r7
wwPd7p1WwALTscwCzd1Crbjy8a2OQ7ZHGC6MLau+LeoNPE0c+uH3tNLloTAvSG
xtUAHfwFa4rM6vLzs/ejJ4ImboI8i4uIA
-----END PUBLIC KEY-----
```

```
nx9500-6C8809#show crypto key rsa
#            KEY NAME         KEY LENGTH
#          #               KEY LENGTH
1          ting                   2048
2          default_rsa_key       2048
```

```
nx9500-6C8809#show crypto pkp trustpoints all
Trustpoint Name: default-trustpoint (self signed)
CRL present: no
Server Certificate details:
  Key used: default_rsa_key
  Serial Number: 051d
  Subject Name: /CN=NX9500-B4-C7-99-6C-88-09
  Issuer Name: /CN=NX9500-B4-C7-99-6C-88-09
  Valid From: Thu Dec  5 04:15:59 2013 UTC
  Valid Until: Sun Dec  3 04:15:59 2023 UTC
```

```
nx9500-6C8809>show crypto cmp request status
CMP Request Status: ir-req-reset
```
### 6.1.16 database

**show commands**

Displays database-related statistics and status

Supported in the following platforms:
- Service Platforms — NX9000, NX9500, NX9510

**Syntax**

`show database [statistics|status] {on <DEVICE-NAME>}`

**Parameters**

- `show database [statistics|status] {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>database</th>
<th>Displays database-related statistics and status</th>
</tr>
</thead>
<tbody>
<tr>
<td>statistics</td>
<td>Displays database-related statistics, such as name of the database (NSight or captive portal), data size, storage size, free disk space available etc.</td>
</tr>
<tr>
<td>status</td>
<td>Displays database status, such as online time.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays database-related information on a specified device</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9510-6C8A5C# show database status
--------------------------------------------------------------------------------
MEMBER     STATE                  ONLINE TIME
--------------------------------------------------------------------------------
localhost (self) PRIMARY               1 hours 31 min 54 sec
--------------------------------------------------------------------------------
nx9510-6C8A5C#

nx9510-6C8A5C# show database statistics
--------------------------------------------------------------------------------
DATABASE   FILE SIZE   STORAGE SIZE   DATA SIZE   INDEX SIZE     DISK FREE
--------------------------------------------------------------------------------
mart       64M         3.0M           784.2k      790.5k       597.2G
--------------------------------------------------------------------------------
nx9510-6C8A5C#
```
6.1.17 device-upgrade

show commands

Displays device firmware upgradation information for devices adopted by a wireless controller or access point

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
show device-upgrade [history|load-image-status|status|versions]
show device-upgrade [history {on <DOMAIN-NAME>}|load-image-status|
versions {on <DEVICE-OR-DOMAIN-NAME>}
show device-upgrade status {on {[<DOMAIN-NAME>]|rf-domain-manager]}
summary {on <DOMAIN-NAME>}}
```

Parameters

- `show device-upgrade [history {on <DOMAIN-NAME>}|load-image-status|versions {on <DEVICE-OR-DOMAIN-NAME>}]`
- `show device-upgrade status {on {[<DOMAIN-NAME>]|rf-domain-manager]}
summary {on <DOMAIN-NAME>}}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>device-upgrade</code></td>
<td>Displays device upgrade information based on the parameters passed</td>
</tr>
<tr>
<td><code>history {on &lt;DOMAIN-NAME&gt;}</code></td>
<td>Displays device upgrade history</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DOMAIN-NAME&gt; – Optional. Displays upgrade history for all devices within a specified RF Domain. Specify the RF Domain name.</td>
</tr>
<tr>
<td><code>load-image-status</code></td>
<td>Displays firmware image loading status. The output displays the &lt;DEVICE&gt; image loading status in percentage.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td><code>#show device-upgrade load-image-status</code></td>
</tr>
<tr>
<td></td>
<td>Download of ap81xx firmware file is 47 percent complete</td>
</tr>
<tr>
<td><code>versions {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</code></td>
<td>Displays firmware image versions</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays firmware image versions loaded on specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>
| `show device-upgrade status {on {[<DOMAIN-NAME>]|rf-domain-manager]}
summary {on <DOMAIN-NAME>}}` | Optional. Displays in progress upgrade status of all devices within a specified RF Domain, or all devices upgraded by the RF Domain manager. Use this option to view upgrade status of multiple devices. |
|                               | • <DOMAIN-NAME> – Specify the RF Domain name.                                                         |
|                               | • rf-domain-manager – Select to view devices upgraded by the RF Domain manager.                       |

```
**SHOW COMMANDS 6-35**

<table>
<thead>
<tr>
<th>summary</th>
<th>Displays a summary of in-progress upgrade processes</th>
</tr>
</thead>
</table>
| {on <DOMAIN-NAME>} | • on <DOMAIN-NAME> – Optional. Displays in-progress upgrade processes within a specified RF Domain  
• <DOMAIN-NAME> – Specify the RF Domain name. |

**Examples**

```
rfs7000-37FABE#show device-upgrade versions
```

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>DEVICE-TYPE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs7000-37FABE</td>
<td>ap621</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap622</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap650</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6511</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6521</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6522</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6532</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6562</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap71xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7502</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7522</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7532</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7562</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap81xx</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap82xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>rfs4000</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>rfs6000</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>rfs7000</td>
<td>none</td>
</tr>
</tbody>
</table>

```
rfs7000-37FABE#device-upgrade load-image rfs6000 ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W58/RFS6000-LEAN.img
```

```
rfs7000-37FABE#device-upgrade load-image ap81xx ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W58/AP81XX.img
```

```
rfs7000-37FABE#show device-upgrade versions
```

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>DEVICE-TYPE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs7000-37FABE</td>
<td>ap621</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap622</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap650</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6511</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6521</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6522</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6532</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap6562</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap71xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7502</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7522</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7532</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap7562</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap81xx</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>ap82xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>rfs4000</td>
<td>none</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>rfs6000</td>
<td>5.8.1.0-035B</td>
</tr>
<tr>
<td>rfs7000-37FABE</td>
<td>rfs7000</td>
<td>none</td>
</tr>
</tbody>
</table>

```
rfs7000-37FABE#```
rfs7000-37FABE# show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0

---

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>STATE</th>
<th>UPGRADE TIME REBOOT</th>
<th>TIME PROGRESS RETRIES</th>
<th>LAST UPDATE ERROR</th>
<th>UPGRADED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs6000-81742D</td>
<td>downloading</td>
<td>immediate</td>
<td>immediate 43</td>
<td>-</td>
<td>rfs7000-37FABE</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#

rfs7000-37FABE# show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 1
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0

---

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>STATE</th>
<th>UPGRADE TIME REBOOT</th>
<th>TIME PROGRESS RETRIES</th>
<th>LAST UPDATE ERROR</th>
<th>UPGRADED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs6000-81742D</td>
<td>rebooting</td>
<td>immediate</td>
<td>immediate 0</td>
<td>0</td>
<td>rfs7000-37FABE</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#

rfs7000-37FABE# show device-upgrade history

---

<table>
<thead>
<tr>
<th>Device</th>
<th>Result</th>
<th>Time</th>
<th>Retries</th>
<th>Upgraded-by</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2014-11-17 02:42:27</td>
<td>0</td>
<td>rfs7000-37FABE</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2015-01-16 01:19:36</td>
<td>0</td>
<td>rfs7000-37FABE</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2015-05-10 22:49:21</td>
<td>0</td>
<td>rfs7000-37FABE</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2014-11-30 21:54:11</td>
<td>0</td>
<td>rfs7000-37FABE</td>
</tr>
<tr>
<td>rfs6000-81742D</td>
<td>done</td>
<td>2015-04-16 06:40:14</td>
<td>0</td>
<td>rfs7000-37FABE</td>
</tr>
</tbody>
</table>

--More--

rfs7000-37FABE#
### 6.1.18 dot1x

> **show commands**

Displays dot1x information on interfaces

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Supported in the following platforms:

- **Access Points** — AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7532, AP7562, AP81XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524

**NOTE:** Dot.1x supplicant configuration is supported on the following platforms:

- **Access Points** — AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX6524

**NOTE:** Dot.1x authenticator configuration is supported on the following platforms:

- **Access Points** — ES6510, AP6511, AP6522, AP6532, AP6562, AP71XX, AP81XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524

#### Syntax

```
show dot1x {all | interface | on}
show dot1x {all {on <DEVICE-NAME>} | on <DEVICE-NAME>}
show dot1x {interface {<INTERFACE-NAME>|ge <1-4}|port-channel <1-2>} {on <DEVICE-NAME>}
```

#### Parameters

- **show dot1x {all | interface | on}**
  - Optional. Displays dot1x information for all interfaces
  - **<DEVICE-NAME>** — Specify the name of the AP, wireless controller, or service platform.

- **show dot1x {all {on <DEVICE-NAME>} | on <DEVICE-NAME>}**
  - Optional. Displays dot1x information for all interfaces on a specified device
  - **<DEVICE-NAME>** — Specify the name of the AP, wireless controller, or service platform.

- **show dot1x {interface {<INTERFACE-NAME>|ge <1-4}|port-channel <1-2>} {on <DEVICE-NAME>}}**
  - Optional. Displays dot1x information for interfaces on a specified device
  - **<DEVICE-NAME>** — Specify the name of the AP, wireless controller, or service platform.

- **show dot1x {interface {<INTERFACE-NAME>|ge <1-4}|port-channel <1-2>} {on <DEVICE-NAME>}}**
  - Optional. Displays dot1x information for a specified interface or interface type

- **<INTERFACE-NAME>**
  - Displays dot1x information for the layer 2 (Ethernet port) interface specified by the `<INTERFACE-NAME>` parameter
ge <1-4> | Displays `dot1x` for a specified GigabitEthernet interface
| • <1-4> – Select the interface index from 1 - 4.

| port-channel <1-2> | Displays `dot1x` for a specified port channel interface
| • <1-2> – Select the interface index from 1 - 2.

| on <DEVICE-NAME> | The following keywords are common to all of the above parameters:
| • on <DEVICE-NAME> – Optional. Displays `dot1x` interface information on a specified device
| • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

**Examples**

```
rfs7000-37FABE(config)#show dot1x all
SysAuthControl is disabled
Guest-Vlan is disabled
AAA-Policy is none

Dot1x info for interface GE1
-----------------------------------
Supplicant MAC N/A
Auth SM State = FORCE AUTHORIZED
Bend SM State = REQUEST
Port Status = AUTHORIZED
Host Mode = SINGLE
Auth Vlan = None
Guest Vlan = None

Dot1x info for interface GE2
-----------------------------------
Supplicant MAC N/A
Auth SM State = FORCE AUTHORIZED
Bend SM State = REQUEST
Port Status = AUTHORIZED
Host Mode = SINGLE
Auth Vlan = None
Guest Vlan = None
--More--
rfs7000-37FABE(config)#
```

```
rfs7000-37FABE(config)#show dot1x interface ge 3
Dot1x info for interface GE3
-----------------------------------
Supplicant MAC N/A
Auth SM State = FORCE AUTHORIZED
Bend SM State = REQUEST
Port Status = AUTHORIZED
Host Mode = SINGLE
Auth Vlan = None
Guest Vlan = None

rfs7000-37FABE(config)#
```
6.1.19 dpi

Displays **Deep Packet Inspection (DPI)** statistics for all configured and canned applications. DPI is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

RF Domain member devices inspect every byte of each application header packet allowed to pass through the WING managed network. When an application is recognized and classified by the WING application recognition engine, administrator defined actions can be applied to that specific application.

**NOTE:** The `show > dpi` command returns results only if executed on a device that supports DPI and has DPI logging enabled. DPI logging can be enabled either on the device or on the profile applied to the device. For more information, see `dpi`.

Supported in the following platforms:
- Access Points — AP7522, AP7532, AP7562
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
show dpi [app|app-category|application|per-category]
show dpi app wireless-clients stats <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
show dpi [app|app-category] stats [<APPLICATION/APP-CATEGORY-NAME>|all] {on <DEVICE-OR-DOMAIN-NAME>}
show dpi application brief
show dpi per-category stats <APP-CATEGORIES> [bytes-in|bytes-out|total-bytes] {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show dpi app wireless-clients stats <MAC> {<DEVICE-OR-DOMAIN-NAME>}`
  - Displays application-related statistics for all or a specified wireless clients
  - `<MAC>` – Displays statistics for a specified wireless client. Specify the client’s MAC address.

- `on <DEVICE-OR-DOMAIN-NAME>`
  - Optional. Displays statistical data on a specified device or RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the access point, wireless controller, service platform, or RF Domain.

- `show dpi [app|app-category] stats [<APPLICATION/APP-CATEGORY-NAME>|all] {on <DEVICE-OR-DOMAIN-NAME>}`
  - Displays statistics for a application or application category
  - `<app>` – Displays statistics for a specified application or all applications
  - `<app-category>` – Displays statistics for a specified application category or all categories.

**Note:** The applications are the RF Domain member allowed applications whose data (bytes) are passing through the WING managed network. And, the application categories are existing WING or user defined application groups (video, streaming, mobile, audio etc.) that assist administrators to permit or deny forwarding of application data.
| **<APPLICATION/APP-CATEGORY-NAME>|all>** | This parameter is common to the ‘app’ and ‘app-category’ keywords.  
• `<APPLICATION/APP-CATEGORY-NAME>` – Displays statistics for a specified application or application category, depending on the option selected in the previous step. Specify the application name or application category name.  
• all – Displays statistics for all application or application category, depending on the option selected in the previous step |
| **on <DEVICE-OR-DOMAIN-NAME>** | Optional. Displays statistical data on a specified device or RF Domain  
• `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the access point, wireless controller, service platform, or RF Domain. |

- **show dpi application brief**

| dpi application brief | Displays a brief summary of applications their status and configuration |

- **show dpi per-category stats <APP-CATEGORIES> [bytes-in|bytes-out|total-bytes] \{on <DEVICE-OR-DOMAIN-NAME>\}**

| dpi per-category stats | Displays statistics for the top ten applications based on the application category and the Sort ID specified. The Sort ID options are: bytes-in, bytes-out or total-bytes. |
| <APP-CATEGORIES> | Specify the application category name. The system displays statistics for the top ten applications in this category. |
| [bytes-in|bytes-out|total-bytes] | Filters and displays statistical data (for the top ten RF Domain member applications in the category specified in the previous step) based on the Sort ID selected.  
• bytes-in – Displays total data bytes uploaded through the RF Domain member WiNG managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).  
• bytes-out – Displays total data bytes downloaded through the RF Domain member WiNG managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).  
• total-bytes – Displays total data bytes (uploaded and downloaded) through the RF Domain member WiNG managed network. These are only the administrator allowed applications approved for proliferation within the RF Domain member device. |
| **on <DEVICE-OR-DOMAIN-NAME>** | Optional. Displays statistical data on a specified device or RF Domain  
• `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the access point, wireless controller, service platform, or RF Domain. |
Examples

nx9500-6C8809>show dpi application brief
  1-clickshare-com
      This application recognizes DirectDownloadLink 1-clickshare traffic
      Application Category : filetransfer
      Predefined Application : Yes
  1-upload-com
      This application recognizes DirectDownloadLink 1-upload-com traffic
      Application Category : filetransfer
      Predefined Application : Yes
  1-upload-to
      This application recognizes DirectDownloadLink 1-upload-to traffic
      Application Category : filetransfer
      Predefined Application : Yes
  10upload-com
      This application recognizes DirectDownloadLink 10upload-com traffic
      Application Category : filetransfer
      Predefined Application : Yes
  123upload-pl
      This application recognizes DirectDownloadLink 123upload-pl traffic
--More--
nx9500-6C8809>
6.1.20 environmental-sensor

Displays environmental sensor’s recorded data. The environmental sensor has to be enabled and configured in order to collect data related to humidity, light, motion, and temperature.

For more information on enabling and configuring environmental sensor settings, see environmental-sensor.

**NOTE:** The environmental sensor is supported only on an AP8132. When executed on any controller (other than an AP8132), the `show > environmental-sensor > <parameters>` command displays environmental-sensor details for adopted AP8132s (if any).

Supported in the following platforms:
- Access Points — AP8132

**Syntax**

```plaintext
show environmental-sensor [history|humidity|light|motion|summary|temperature|version]
show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}
show environmental-sensor [humidity|light|motion|summary|temperature|version]
```

**Parameters**

- `show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}`

| environmental-sensor history | Displays environmental sensor history once in every hour, 20 minutes, or 24 hours.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1-hour</td>
<td>Optional. Displays environmental sensor history once in every 1 (one) hour</td>
</tr>
<tr>
<td>20-minute</td>
<td>Optional. Displays environmental sensor history once in every 20 minutes</td>
</tr>
<tr>
<td>24-hour</td>
<td>Optional. Displays environmental sensor history once in every 24 hours</td>
</tr>
</tbody>
</table>

- `show environmental-sensor [humidity|light|motion|summary|temperature|version]`

| environmental-sensor         | Displays environmental sensor’s recorded data, based on the parameters passed. The system displays the specified recorded data.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>humidity</td>
<td>Displays the minimum, average, and maximum humidity recorded</td>
</tr>
<tr>
<td>light</td>
<td>Displays the minimum, average, and maximum light recorded</td>
</tr>
<tr>
<td>motion</td>
<td>Displays the minimum, average, and maximum motion recorded</td>
</tr>
<tr>
<td>temperature</td>
<td>Displays the minimum, average, and maximum temperature recorded</td>
</tr>
<tr>
<td>version</td>
<td>Displays the hardware and firmware versions</td>
</tr>
<tr>
<td>summary</td>
<td>Displays a summary of the data recorded at following intervals:</td>
</tr>
</tbody>
</table>

---
Examples

ap8132-711728# show environmental-sensor summary
Maat Device uptime: 0 days 15:25:11
ERROR: Maat device is offline!
threshold polling-interval: 5
historical data polled 0 times per 2-minutes interval since Maat online

motion-sensor: Enabled(Demo)
current value: 0 detected
motion detected

20-minute 0
1-hour 0
6-hour 0
24-hour 0

temperature-sensor: Enabled(Demo)
current value: -40.00 deg. C

20-minute 0/0/0
1-hour 0/0/0
6-hour 0/0/0
24-hour 0/0/0

light-sensor: Enabled
threshold-high:+400.00 threshold-low:+200.00 holdtime:11
action radio-shutdown: radio-1 and radio-2
light-on:1
light-on/off event sent:0/0
current value: 0.00 lux

20-minute 0/0/0
1-hour 0/0/0
6-hour 0/0/0
24-hour 0/0/0

humidity-sensor: Enabled(Demo)
current value: 0.00 %

20-minute 0/0/0
1-hour 0/0/0
6-hour 0/0/0
24-hour 0/0/0

ap8132-711728#

ap8132-711634# show env-sensor history
Current Time: 2015-06-20 14:08:01 UTC

<table>
<thead>
<tr>
<th>Sample-Interval</th>
<th>Motion</th>
<th>Temperature (deg. C)</th>
<th>Light (lux)</th>
<th>Humidity (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20-minute</td>
<td>1</td>
<td>64/65/66</td>
<td>77/80</td>
<td>58/60/61</td>
</tr>
<tr>
<td>1-hour</td>
<td>24</td>
<td>63/67/70</td>
<td>75/81</td>
<td>57/59/61</td>
</tr>
<tr>
<td>6-hour</td>
<td>128</td>
<td>60/62/69</td>
<td>71/79</td>
<td>52/56/71</td>
</tr>
<tr>
<td>24-hour</td>
<td>188</td>
<td>54/58/70</td>
<td>15/45</td>
<td>49/57/73</td>
</tr>
</tbody>
</table>

ap8132-711634#
### Show Env-Sensor History 20-Min

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Motion</th>
<th>Temperature</th>
<th>Light</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-11-20 13:51:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 13:53:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 13:55:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
<td>58</td>
</tr>
<tr>
<td>2015-11-20 13:57:35 UTC</td>
<td>1</td>
<td>66</td>
<td>80</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 13:59:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 14:02:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:03:35 UTC</td>
<td>0</td>
<td>64</td>
<td>79</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:05:35 UTC</td>
<td>2</td>
<td>66</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:07:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
<td>61</td>
</tr>
<tr>
<td>2015-11-20 14:09:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
<td>61</td>
</tr>
</tbody>
</table>

### Show Env-Sensor History 1-Hr

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Motion</th>
<th>Temperature</th>
<th>Light</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-11-20 13:51:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 13:53:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 13:55:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
<td>58</td>
</tr>
<tr>
<td>2015-11-20 13:57:35 UTC</td>
<td>1</td>
<td>66</td>
<td>80</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 13:59:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:01:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:03:35 UTC</td>
<td>0</td>
<td>64</td>
<td>79</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:05:35 UTC</td>
<td>2</td>
<td>66</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:07:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
<td>61</td>
</tr>
<tr>
<td>2015-11-20 14:09:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
<td>61</td>
</tr>
<tr>
<td>2015-11-20 14:42:35 UTC</td>
<td>0</td>
<td>65</td>
<td>81</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 14:43:35 UTC</td>
<td>0</td>
<td>64</td>
<td>80</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-20 14:45:35 UTC</td>
<td>3</td>
<td>66</td>
<td>80</td>
<td>60</td>
</tr>
</tbody>
</table>

### Show Env-Sensor History 24-Hr

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Motion</th>
<th>Temperature</th>
<th>Light</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-11-20 10:10:20 UTC</td>
<td>27</td>
<td>66</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 10:30:20 UTC</td>
<td>17</td>
<td>66</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 10:50:20 UTC</td>
<td>17</td>
<td>66</td>
<td>81</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 11:10:20 UTC</td>
<td>25</td>
<td>66</td>
<td>81</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 11:30:20 UTC</td>
<td>24</td>
<td>66</td>
<td>81</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-20 11:50:20 UTC</td>
<td>26</td>
<td>66</td>
<td>81</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-21 08:10:20 UTC</td>
<td>9</td>
<td>65</td>
<td>80</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-21 08:30:20 UTC</td>
<td>7</td>
<td>65</td>
<td>80</td>
<td>59</td>
</tr>
<tr>
<td>2015-11-21 08:50:20 UTC</td>
<td>12</td>
<td>65</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-21 09:10:20 UTC</td>
<td>10</td>
<td>65</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-21 09:30:20 UTC</td>
<td>15</td>
<td>65</td>
<td>80</td>
<td>60</td>
</tr>
<tr>
<td>2015-11-21 09:50:20 UTC</td>
<td>19</td>
<td>66</td>
<td>80</td>
<td>60</td>
</tr>
</tbody>
</table>
6.1.21 event-history

Display event history report

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
show event-history [on <DEVICE-OR-DOMAIN-NAME>]
```

Parameters

- show event-history [on <DEVICE-OR-DOMAIN-NAME>]

Examples

```
rfs7000-6DCD4B(config)#show event-history
EVENT HISTORY REPORT
Generated on '2015-04-20 01:06:51 UTC' by 'admin'

2015-04-20 01:06:40     rfs7000-6DCD4B  SYSTEM     LOGIN                Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-04-20 00:40:09     ap8132-711728  SYSTEM     LOGIN                Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-04-20 00:39:53     rfs6000-81742D  SYSTEM     LOGIN                Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-04-20 00:39:41     rfs7000-6DCD4B  SYSTEM     LOGIN                Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2015-04-19 23:17:43     ap8132-711728  NSM        DHCPIP               Interface vlan1 acquired IP address 10.2.0.99/24 via DHCP
2015-04-19 23:17:43     ap8132-711728  NSM        DHCPDEFRT            Default route with gateway 10.2.0.1 learnt via DHCP
2015-04-19 18:40:22     rfs6000-81742D  NSM        DHCPIP               Interface vlan1 acquired IP address 10.2.0.100/24 via DHCP
2015-04-19 18:40:22     rfs6000-81742D  NSM        DHCPDEFRT            Default route with gateway 10.2.0.1 learnt via DHCP
2015-04-19 11:17:41     ap8132-711728  NSM        DHCPIP               Interface vlan1 acquired IP address 10.2.0.99/24 via DHCP
2015-04-19 11:17:41     ap8132-711728  NSM        DHCPDEFRT            Default route with gateway 10.2.0.1 learnt via DHCP
--More--
rfs7000-6DCD4B(config)#
```
### 6.1.22 event-system-policy

#### show commands

Displays detailed event system policy configuration

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>
```

**Parameters**

- `show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>`

<table>
<thead>
<tr>
<th>event-system-policy</th>
<th>Displays event system policy configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays configuration for a specified policy</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed configuration for a specified policy</td>
</tr>
<tr>
<td>&lt;EVENT-SYSTEM-POLICY-NAME&gt;</td>
<td>Specify the event system policy name.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#show event-system-policy config testpolicy
-----------------------------------------------------------------------
MODULE   EVENT                SYSLOG   SNMP   FORWARD    EMAIL
-----------------------------------------------------------------------
aaa      radius-discon-msg    on       on      on         default
-----------------------------------------------------------------------
rfs7000-37FABE(config)#
```
### 6.1.23 ex3500

#### show commands
Displays EX3500-related statistical data

Supported in the following platforms:
- Wireless Controllers — RFS7000
- Service Platforms — NX7500, NX9500

#### Syntax

```
show ex3500 [dir|interfaces|system|upgrade|version|whichboot]
show ex3500 dir {boot-rom|config|on|opcode} {<FILE-NAME>} {on <EX3500-DEVICE-NAME>}
show ex3500 interfaces counters [ether-like stats|ethernet <1-1> <1-52>| ext-if-table stats|if-table stats|portUtil stats|rmon stats] {on <EX3500-DEVICE-NAME>}
show ex3500 [system|upgrade|version|whichboot] {on <EX3500-DEVICE-NAME>}
```

#### Parameters

- **show ex3500 dir {boot-rom|config|on|opcode} {<FILE-NAME>} {on <EX3500-DEVICE-NAME>}
  - **<FILE-NAME>** Displays the contents of a specified file identified by the `<FILE-NAME>` keyword. This is the name of configuration file or code image.
  - **on <EX3500-DEVICE-NAME>** Optional. Executes the command on a specified EX3500 device
    - `<DEVICE-NAME>` – Specify the device’s name.

- **show ex3500 interfaces counters [ether-like stats|ethernet <1-1> <1-52>| ext-if-table stats|if-table stats|portUtil stats|rmon stats] {on <EX3500-DEVICE-NAME>}
  - **ether-like stats** Displays Managed Information Base (MIB) object statistics for Ethernet-like interfaces
  - **ethernet <1-1> <1-52>** Displays the Ethernet port statistics based on the unit identifier and port number selected
    - `<1-1>` – Specify the EX3500 unit’s identifier from 1 - 1.
    - `<1-52>` – Specify the port number from 1 - 52. This range varies for the EX3524 (1-28) and EX3548 (1-52) devices.
    - **Note:** This option displays the following for the selected Ethernet interface:
      - extended interface table stats, interface table stats, port utilization information, and remote monitoring stats.
  - **ext-if-table stats** Displays only the extended interface table statistics
if-table stats | Displays only the interface table statistics
---|---
portUtil stats | Displays only the port utilization information
---|---
rmon stats | Displays only remote monitoring (RMon) statistics
---|---
on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device
• <DEVICE-NAME> – Specify the device's name.
---|---

Examples

```
nx9500-6C8809#show ex3500 interfaces counters ethernet 1 17
Ethernet 1/ 17
====== IF table Stats ======
2166458 Octets Input
14734059 Octets Output
14707 Unicast Input
19806 Unicast Output
0 Discard Input
0 Discard Output
0 Error Input
0 Error Output
0 Unknown Protocols Input
0 QLen Output
====== Extended Iftable Stats ======
23 Multi-cast Input
5526 Multi-cast Output
170 Broadcast Input
11 Broadcast Output
====== Ether-like Stats ======
0 Alignment Errors
0 FCS Errors
0 Single Collision Frames
0 Multiple Collision Frames
0 SQE Test Errors
0 Deferred Transmissions
0 Late Collisions
0 Excessive Collisions
0 Internal Mac Transmit Errors
0 Internal Mac Receive Errors
0 Frames Too Long
0 Carrier Sense Errors
0 Symbol Errors
0 Pause Frames Input
0 Pause Frames Output
====== RMON Stats ======
0 Drop Events
16900558 Octets
```
40243 Packets
170 Broadcast PKTS
23 Multi-cast PKTS
0 Undersize PKTS
0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
21065 Packet Size <= 64 Octets
3805 Packet Size 65 to 127 Octets
2448 Packet Size 128 to 255 Octets
797 Packet Size 256 to 511 Octets
2941 Packet Size 512 to 1023 Octets
9187 Packet Size 1024 to 1518 Octets

===== Port Utilization (recent 300 seconds) =====
0 Octets Input in kbits per second
0 Packets Input per second
0.00 % Input Utilization
0 Octets Output in kbits per second
0 Packets Output per second
0.00 % Output Utilization

nx9500-6C8809#
6.1.24 extdev

▶ show commands

Displays external device (T5 or EX3500) configuration error history

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000, NX9500, NX9510

Syntax
show extdev error history {on <T5/EX3500-DEVICE-NAME>}

Parameters
- show extdev error history {on <T5/EX3500-DEVICE-NAME>}

<table>
<thead>
<tr>
<th>extdev error history</th>
<th>Displays external device error history. This command is applicable only to the external devices T5, and EX3500 series switch. Use this command to view configuration error history for all or a specified external device adopted and managed by a WiNG NX9500 series service platform.</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;T5/EX3500-DEVICE-NAME&gt;</td>
<td>Optional. Displays configuration error history on a specified T5 or EX3500 device&lt;br&gt;• &lt;T5/EX3500-DEVICE-NAME&gt; – Specify the name of the device.</td>
</tr>
</tbody>
</table>

Examples
nx9500-6C8809# show extdev error history on t5-ED5EAC<br>%% No History for this device<br>nx9500-6C8809#
6.1.25 file

SHOW COMMANDS 6-51

This command is not available in the USER EXEC mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
show file [information <FILE>|systems]
```

Parameters

- show file [information <FILE>|systems]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>Displays file system related information</td>
</tr>
<tr>
<td>information &lt;FILE&gt;</td>
<td>Displays information for a specified file</td>
</tr>
<tr>
<td>&lt;FILE&gt;</td>
<td>Specify the file name.</td>
</tr>
<tr>
<td>systems</td>
<td>Lists all file systems present in the system</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809#show file systems
File Systems:

    Size(Mb)   Free(Mb)  Use%   Type    Prefix
    23471      22107     5    flash   nvram:
    117344     111150    5    flash   flash:
    644901     609787    5    flash   internal (/vms)
nx9500-6C8809#
```

```
nx9500-6C8809#show file information
flash:/ nvram:/ startup-config system:/ running-config
```

```
nx9500-6C8809#show file information flash:
flash:/
  type is directory
```

```
nx9500-6C8809#
```
6.1.26 file-sync

show commands

Displays file synchronization settings and status on a controller.

The `file-sync` command syncs EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adoptee AP6522/AP6562 client-bridge access points. The `show > file-sync` command displays information related to this process.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

Syntax

```
show file-sync [configuration|history|load-file-status|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

- `file-sync` Displays the following file-synchronization related information: configuration, history, load-file-status, and status
- `configuration` Displays the following file-synchronization configuration details:
  - automatic file-syncing enabled or disabled. The default setting is disabled.
  - Number of access points the certificate can be simultaneously uploaded. The default is 10.
  - Scheduled certificate upload, if any, details, such time and date of upload.
- `history` Displays file synchronization history. Use this option to view statistical data relating to client-bridge certificate synchronization between staging controller and adoptee access points. When executed, a list of all certificate transfers made to the client-bridge is displayed, with the latest transfer listed at the top.
- `load-file-status` Displays the status of PKCS#12 certificate upload to the controller. Use this command to view the status of a in-progress certificate upload.
- `status` Displays status of the PKCS#12 certificate synchronization between the controller and the client-bridge access point.

- `on <DEVICE-OR-DOMAIN-NAME>` Optional. Displays file synchronization settings and status on a specified device or RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` — Specify the name of the controller, service platform, or RF Domain.
Examples

nx9500-6C8809# show file-sync configuration
File Sync Configuration Information
   Auto : Disabled
   Simultaneous Upload Count : 128
nx9500-6C8809#

nx9500-6C8809# show file-sync load-file-status
Download of wireless_bridge certificate is complete
nx9500-6C8809#

nx9500-6C8809# show file-sync history

--------------------------------------------------------------------------------------------
| AP       | RESULT          | TIME    | RETRIES  | SYNCED-BY         | LAST-SYNC-ERROR                      |
--------------------------------------------------------------------------------------------
| AP6522-491220 failed | 2015-05-27 01:37:32 3 B4-C7-99-6C-88-09 | Start Upload failed, retries = 3 |
| AP6522-491220 failed | 2015-05-27 01:42:29 3 B4-C7-99-6C-88-09 | Start Upload failed, retries = 3 |
| AP6522-491220 failed | 2015-05-27 01:45:22 3 B4-C7-99-6C-88-09 | Start Upload failed, retries = 3 |
| ME733ANACBMOT21 done | 2015-05-27 02:02:51 0 B4-C7-99-6C-88-09 | - |
--------------------------------------------------------------------------------------------

nx9500-6C8809#
6.1.27 firewall

■ show commands
Displays wireless firewall information, such as Dynamic Host Configuration Protocol (DHCP) snoop table entries, denial of service statistics, active session summaries etc.

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9600

Syntax

show firewall [dhcp|dos|flows|neighbors]

show firewall [dhcp snoop-table|dos stats] {on <DEVICE-NAME>}

show firewall flows {filter|management|on|stats|wireless-client}

show firewall flows {filter} {dir|dst port <1-65535>|ether|flow-type|icmp|icmpv6|igmp|ip|ipv6|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp}

show firewall flows {management} {on <DEVICE-NAME>}{stats} {on <DEVICE-NAME>}

show firewall neighbors snoop-table {on <DEVICE-NAME>}

Parameters

• show firewall [dhcp snoop-table|dos stats] {on <DEVICE-NAME>}

| firewall dhcp snoop-table | Displays DHCP snoop table entries
|---------------------------|----------------------------------
|                           | • snoop-table – Displays DHCP snoop table entries
|                           | DHCP snooping acts as a firewall between non-trusted hosts and the DHCP server.
|                           | Snoop table entries contain MAC address, IP address, lease time, binding type, and
|                           | interface information of non-trusted interfaces.

| dos stats | Displays Denial of Service (DoS) statistics
|-----------|----------------------------------
|           | Note: This option is not available in the User Exec mode.

| on <DEVICE-NAME> | The following keyword is common to the ‘DHCP snoop table’ and ‘DoS stats’ parameters:
|------------------|----------------------------------
|                   | • on <DEVICE-NAME> – Optional. Displays snoop table entries, or DoS stats on a
|                   | specified device
|                   | • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or
|                   | service platform.

• show firewall flows {filter} {dir|dst|ether|flow-type|icmp|icmpv6|igmp|ip|ipv6|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp}

| firewall flows | Notifies a session has been established
|----------------|----------------------------------
| filter | Optional. Defines additional firewall flow filter parameters

|-----------------------------------|----------------------------------
| wired-wired – Wired to wired flows
| wired-wireless – Wired to wireless flows
| wireless-wired – Wireless to wired flows
| wireless-wireless – Wireless to wireless flows
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst port <code>&lt;1-65535&gt;</code></td>
<td>Optional. Matches the destination port with the specified port&lt;br&gt;• port <code>&lt;1-65535&gt;</code> – Specifies the destination port number from 1 - 65535</td>
</tr>
<tr>
<td>ether <code>[dst &lt;MAC&gt;]&lt;br&gt;host &lt;MAC&gt; src &lt;MAC&gt; vlan &lt;1-4094&gt;]</code></td>
<td>Optional. Displays Ethernet filter options&lt;br&gt;• dst &lt;MAC&gt; – Matches only the destination MAC address&lt;br&gt;• host &lt;MAC&gt; – Matches flows containing the specified MAC address&lt;br&gt;• src &lt;MAC&gt; – Matches only the source MAC address&lt;br&gt;• vlan &lt;1-4094&gt; – Matches the VLAN number of the traffic with the specified value. Specify a value from 1- 4094.</td>
</tr>
<tr>
<td>flow-type `[bridged</td>
<td>natted</td>
</tr>
<tr>
<td>icmp `{code</td>
<td>type}`</td>
</tr>
<tr>
<td>icmpv6 `{code</td>
<td>type}`</td>
</tr>
<tr>
<td>igmp</td>
<td>Optional. Matches Internet Group Management Protocol (IGMP) flows</td>
</tr>
<tr>
<td>ip <code>[dst &lt;IP&gt;]&lt;br&gt;host &lt;IP&gt; proto &lt;0-254&gt; src &lt;IP&gt;]</code></td>
<td>Optional. Filters firewall flows based on the IPv4 parameters passed&lt;br&gt;• dst &lt;IP&gt; – Matches destination IP address&lt;br&gt;• host &lt;IP&gt; – Matches flows containing IPv4 address&lt;br&gt;• proto &lt;0-254&gt; – Matches the IPv4 protocol number with the specified number&lt;br&gt;• src &lt;IP&gt; – Matches source IP address</td>
</tr>
<tr>
<td>ipv6 <code>[dst &lt;IPv6&gt; host &lt;IPv6&gt; proto &lt;0-254&gt; src &lt;IPv6&gt;]</code></td>
<td>Optional. Filters firewall flows based on the IPv6 parameters passed&lt;br&gt;• dst &lt;IPv6&gt; – Matches destination IPv6 address&lt;br&gt;• host &lt;IPv6&gt; – Matches flows containing IPv6 address&lt;br&gt;• proto &lt;0-254&gt; – Matches the IPv6 protocol number with the specified number&lt;br&gt;• src &lt;IPv6&gt; – Matches source IPv6 address</td>
</tr>
<tr>
<td>max-idle <code>&lt;1-4294967295&gt;</code></td>
<td>Optional. Filters firewall flows idle for at least the specified duration. Specify a max-idle value from 1 - 4294967295 bytes.</td>
</tr>
<tr>
<td>min-bytes <code>&lt;1-4294967295&gt;</code></td>
<td>Optional. Filters firewall flows with at least the specified number of bytes. Specify a min-bytes value from 1 - 4294967295 bytes.</td>
</tr>
<tr>
<td>min-idle <code>&lt;1-4294967295&gt;</code></td>
<td>Optional. Filters firewall flows idle for at least the specified duration. Specify a min-idle value from 1 - 4294967295 bytes.</td>
</tr>
<tr>
<td>min-pkts <code>&lt;1-4294967295&gt;</code></td>
<td>Optional. Filters firewall flows with at least the given number of packets. Specify a min-bytes value from 1 - 4294967295 bytes.</td>
</tr>
<tr>
<td>not</td>
<td>Optional. Negates the filter expression selected</td>
</tr>
<tr>
<td>port <code>&lt;1-65535&gt;</code></td>
<td>Optional. Matches either the source or destination port. Specify a port from 1 - 65535.</td>
</tr>
</tbody>
</table>
src <1-65535> | Optional. Matches only the source port with the specified port. Specify a port from 1 - 65535.
tcp | Optional. Matches TCP flows
udp | Optional. Matches UDP flows

- show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}|wireless-client <MAC>|on <DEVICE-NAME>}

**Examples**

```
rfs7000-6DCD4B(config)#show firewall dhcp snoop-table
Snoop Binding <10.2.0.1, 00-00-00-00-00-00, Vlan 1>
Type router, Touched 686539 seconds ago
Snoop Binding <172.18.0.2, B4-C7-99-6D-CD-4B, Vlan 1>
Type switch-SVI, Touched 688432 seconds ago
Snoop Binding <192.168.13.111, B4-C7-99-6D-CD-4B, Vlan 192>
Type switch-SVI, Touched 688431 seconds ago
rfs7000-6DCD4B(config)#
```
rfs7000-6DCD4B(config)#show firewall dos stats

<table>
<thead>
<tr>
<th>ATTACK TYPE</th>
<th>COUNT</th>
<th>LAST OCCURENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp-short-hdr</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>multicast-icmpv6</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>icmp-router-solicit</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>tcp-xmas-scan</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>ascend</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>twinge</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>tcp-post-syn</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>land</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>broadcast-multicast-icmp</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>ftp-bounce</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>spoof</td>
<td>0</td>
<td>Never</td>
</tr>
<tr>
<td>source-route</td>
<td>0</td>
<td>Never</td>
</tr>
</tbody>
</table>

--More--

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show firewall flows management

====== Flow# 1 Summary ======

Forward:
- IPv4 Vlan 192, TCP 192.168.13.10 port 2909 > 192.168.13.111 port 22
- 00-02-B3-28-D1-55 > B4-C7-99-6D-CD-4B, ingress port ge2
- Egress port: <local>, Egress interface: vlan192, Next hop: <local> (B4-C7-99-6D-CD-4B)
- 1451 packets, 116262 bytes, last packet 0 seconds ago

Reverse:
- IPv4 Vlan 192, TCP 192.168.13.111 port 22 > 192.168.13.10 port 2909
- B4-C7-99-6D-CD-4B > 00-02-B3-28-D1-55, ingress port local
- Egress port: ge2, Egress interface: vlan192, Next hop: 192.168.13.10 (00-02-B3-28-D1-55)
- 1284 packets, 148585 bytes, last packet 1 seconds ago
- TCP state: Established
- Flow times out in 1 hour 30 minutes

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show firewall flows stats

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B(config)#
6.1.28 global

show commands

Displays global information for network devices based on the parameters passed

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show global [device-list|domain]

show global device-list {filter {offline|online|rf-domain}}
show global device-list {filter {offline|online}}
show global device-list {filter rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>]}

show global domain managers

Parameters

- show global device-list {filter {offline|online}}

<table>
<thead>
<tr>
<th>global device-list</th>
<th>Displays global information for all network devices. Use the following keywords to specify additional filters: offline, online, and rf-domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter {offline</td>
<td>online}</td>
</tr>
<tr>
<td></td>
<td>• offline – Optional. Displays global information for offline devices only</td>
</tr>
<tr>
<td></td>
<td>• online – Optional. Displays global information for online devices only</td>
</tr>
</tbody>
</table>

- show global device-list {filter rf-domain [<DOMAIN-NAME>|not <DOMAIN-NAME>]}

<table>
<thead>
<tr>
<th>global device-list</th>
<th>Displays global information for all network devices. Use the following keywords to specify additional filters: offline, online, and rf-domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter rf-domain</td>
<td>Optional. Specifies additional filters</td>
</tr>
<tr>
<td>[&lt;DOMAIN-NAME&gt;]</td>
<td>• rf-domain – Optional. Displays global information for all devices in a specified RF Domain</td>
</tr>
<tr>
<td>not &lt;DOMAIN-NAME&gt;</td>
<td>• &lt;DOMAIN-NAME&gt; – Optional. Displays information of all devices within the domain identified by the &lt;DOMAIN-NAME&gt; keyword</td>
</tr>
<tr>
<td></td>
<td>• not &lt;DOMAIN-NAME&gt; – Optional. Displays information of all devices in domains not matching the &lt;DOMAIN-NAME&gt; keyword</td>
</tr>
</tbody>
</table>

- show global domain managers

<table>
<thead>
<tr>
<th>global domain managers</th>
<th>Displays global information for all RF Domains and managers in the network</th>
</tr>
</thead>
</table>
### Examples

```
rfs7000-6DCD4B(config)#show global device-list filter rf-domain default

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>CLUSTER</th>
<th>RF-DOMAIN</th>
<th>ADOPTED-BY</th>
<th>ONLINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-81-74-2D</td>
<td>rfs6000-81742D</td>
<td>rfs6000</td>
<td>default</td>
<td>B4-C7-99-6D-CD-4B</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>B4-C7-99-6D-CD-4B</td>
<td>rfs7000-6DCD4B</td>
<td>rfs7000</td>
<td>default</td>
<td>00-15-70-81-74-2D</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>B4-C7-99-71-17-28</td>
<td>ap8132-711728</td>
<td>ap81xx</td>
<td>default</td>
<td>00-15-70-81-74-2D</td>
<td>online</td>
<td></td>
</tr>
</tbody>
</table>

Total number of clients displayed: 3
```

```
rfs7000-6DCD4B(config)#show global domain managers

<table>
<thead>
<tr>
<th>RF-DOMAIN</th>
<th>MANAGER</th>
<th>HOST-NAME</th>
<th>APS</th>
<th>CLIENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>B4-C7-99-6D-CD-4B</td>
<td>rfs7000-6DCD4B</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Total number of RF-domain displayed: 1
```

rfs7000-6DCD4B(config)#
6.1.29 **gre**

> **show commands**

Displays layer 2 *Generic Routing Encapsulation* (GRE) tunnel traffic flow information

GRE is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show gre info {detail} {(on <DEVICE-NAME>)}`

**Parameters**

- `show gre info {detail} {(on <DEVICE-NAME>)}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gre info</code></td>
<td>Displays GRE tunnel information</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>Optional. Displays GRE tunnel information in detail, such as tunnel state,</td>
</tr>
<tr>
<td></td>
<td>tunnel's remote-end peer device's IP address, session ID of an operational</td>
</tr>
<tr>
<td></td>
<td>tunnel, total number of packets received and transmitted through the tunnel,</td>
</tr>
<tr>
<td></td>
<td>and the number of dropped packets during tunneled exchanges between access</td>
</tr>
<tr>
<td></td>
<td>point and a peer at the remote end of the tunnel.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Executes the command on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the access point, controller, or</td>
</tr>
<tr>
<td></td>
<td>service platform.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx4500-5CFA2B>show gre info
Gre Tunnel info:
  {'No tunnel found': 0}
nx4500-5CFA2B>
```
6.1.30 **guest-registration**

Displays guest registration statistics based on the option and time entered

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

```
show guest-registration [age-range|backup-snapshots|browsers|devices|gender|notification-status|os|social|user-trends|visitors] {on <DEVICE-NAME>}
```

```
show guest-registration backup-snapshots
```

```
show guest-registration [age-range|browsers|devices|gender|os|user-trends|visitors] time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>)}
```

```
show guest-registration client [email|mac|member|mobile|name|time]
```

```
show guest-registration client [email <EMAIL-ADDRESS>|mac <MAC>|member <MEMBER-ID>|mobile <MOBILE-NUMBER>|name <NAME>]
```

```
show guest-registration client time [1-Hour|10-Mins|15-Mins|2-Mins|30-Mins|30-Secs|5-Mins] {(rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>)}
```

```
show guest-registration notification-status
```

```
show guest-registration social time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(facebook|rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>|google)}
```

**Parameters**

- **show guest-registration backup-snapshots**

<table>
<thead>
<tr>
<th>guest-registration</th>
<th>Displays guest registration statistics based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup-snapshots</td>
<td>Displays a list of periodically backed up snapshots of the database. By default, the system maintains a snapshot of the database on a daily basis. <strong>Note:</strong> Use the `service &gt; guest-registration &gt; backup [delete</td>
</tr>
</tbody>
</table>

- **show guest-registration [age-range|browsers|devices|gender|os|user-trends|visitors] time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>)}**

<table>
<thead>
<tr>
<th>guest-registration</th>
<th>Displays guest registration statistics based on the parameters and time entered. Optionally, use the ‘rfdomain’ and/or ‘wlan’ keywords to view guest registration statistics for a specified RF Domain and/or WLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>age-range</td>
<td>Displays the age ranges of logged guest users for a selected time period</td>
</tr>
<tr>
<td>browsers</td>
<td>Displays the browsers used by guest users logged in within a selected time period</td>
</tr>
<tr>
<td>devices</td>
<td>Displays the device types used by guest users logged in within a selected time period</td>
</tr>
<tr>
<td>gender</td>
<td>Displays the gender of guest users logged in within a selected time period</td>
</tr>
<tr>
<td>os</td>
<td>Displays the operating system (OS) of devices logged in within a selected time period</td>
</tr>
<tr>
<td>user-trends</td>
<td>Displays guest user login trends for a selected time period. It displays statistical data, such as number of new users, number of return users, and total of number users.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>visitors</strong></td>
<td>Displays type of visitors logged in within a selected time period</td>
</tr>
</tbody>
</table>
| **time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all]** | Displays guest registration statistics, for a specified time period. The stats displayed depends on the option selected in the previous step. Specify the time period using one of the following options:  
  - 1-Day – Displays previous day’s statistics  
  - 1-Month – Displays previous month’s statistics  
  - 1-Week – Displays previous week’s statistics  
  - 2-Hours – Displays last 2 hours statistics  
  - 30-Mins – Displays last 30 minutes statistics  
  - 5-Hours – Displays last 5 hours statistics  
  - all – Displays statistics from the day the database was created |
| **[rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>]** | Use the following options as additional filters:  
  - <DOMAIN-NAME> – Specify the RF Domain name.  
  - wlan <WLAN-NAME> – Optional. Displays guest registration statistics for a specified WLAN.  
  - <WLAN-NAME> – Specify the WLAN name. |

- **show guest-registration client [email <EMAIL-ADDRESS>|mac <MAC>|member <MEMBER-ID>|mobile <MOBILE-NUMBER>|name <NAME>]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>guest-registration</strong></td>
<td>Displays guest registration statistics based on the parameters and time entered. Optionally, use the ‘rfdomain’ and/or ‘wlan’ keywords to view guest registration statistics for a specified RF Domain and/or WLAN.</td>
</tr>
<tr>
<td><strong>client</strong></td>
<td>Displays statistical data for a specific client. Use the e-mail, mac, member, mobile, name to provide a match criteria.</td>
</tr>
</tbody>
</table>
| **email <EMAIL-ADDRESS>** | Displays statistical data for the client with e-mail address matching the <EMAIL-ADDRESS> parameter  
  - <EMAIL-ADDRESS> – Specify the client’s e-mail address. |
| **mac <MAC>** | Displays statistical data for the client with MAC address matching the <MAC> parameter  
  - <MAC> – Specify the client’s MAC address |
| **member <MEMBER-ID>** | Displays statistical data for the client with member ID matching the <MEMBER-ID> parameter  
  - <MEMBER-ID> – Specify the client’s member ID. |
| **mobile <MOBILE-NUMBER>** | Displays statistical data for the client with mobile number matching the <MOBILE-NUMBER> parameter  
  - <MOBILE-NUMBER> – Specify the client’s mobile number. |
| **name <NAME>** | Displays statistical data for the client with name matching the <NAME> parameter  
  - <NAME> – Specify the client’s name. |


<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>guest-registration</strong></td>
<td>Displays statistics for logged clients. Optionally, use the ‘rfdomain’ and/or ‘wlan’ keywords to view guest registration statistics for a specified RF Domain and/or WLAN.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show client</code></td>
<td>Displays statistical data for all clients logged in within a specified time period</td>
</tr>
<tr>
<td>`time [1-Day</td>
<td>1-Month</td>
</tr>
<tr>
<td></td>
<td>• 1-Day – Displays previous day’s statistics</td>
</tr>
<tr>
<td></td>
<td>• 1-Month – Displays previous month’s statistics</td>
</tr>
<tr>
<td></td>
<td>• 1-Week – Displays previous week’s statistics</td>
</tr>
<tr>
<td></td>
<td>• 2-Hours – Displays last 2 hours statistics</td>
</tr>
<tr>
<td></td>
<td>• 30-Mins – Displays last 30 minutes statistics</td>
</tr>
<tr>
<td></td>
<td>• 5-Hours – Displays last 5 hours statistics</td>
</tr>
<tr>
<td></td>
<td>• all – Displays entire statistics, from the day the database was created</td>
</tr>
<tr>
<td>`[rfdomain &lt;DOMAIN-NAME&gt;</td>
<td>wlan &lt;WLAN-NAME&gt;]`</td>
</tr>
<tr>
<td></td>
<td>• rfdomain &lt;DOMAIN-NAME&gt; – Optional. Displays guest registration statistics for a specified RF Domain.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</td>
</tr>
<tr>
<td></td>
<td>• wlan &lt;WLAN-NAME&gt; – Optional. Displays guest registration statistics for a specified WLAN.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WLAN-NAME&gt; – Specify the WLAN name.</td>
</tr>
<tr>
<td><code>show guest-registration notification-status</code></td>
<td>Displays guest registration notification status</td>
</tr>
<tr>
<td>`show guest-registration social [time [1-1-Day</td>
<td>1-Month</td>
</tr>
<tr>
<td></td>
<td>• 1-Day – Displays previous day’s statistics</td>
</tr>
<tr>
<td></td>
<td>• 1-Month – Displays previous month’s statistics</td>
</tr>
<tr>
<td></td>
<td>• 1-Week – Displays previous week’s statistics</td>
</tr>
<tr>
<td></td>
<td>• 2-Hours – Displays last 2 hours statistics</td>
</tr>
<tr>
<td></td>
<td>• 30-Mins – Displays last 30 minutes statistics</td>
</tr>
<tr>
<td></td>
<td>• 5-Hours – Displays last 5 hours statistics</td>
</tr>
<tr>
<td></td>
<td>• all – Displays the entire database</td>
</tr>
<tr>
<td><code>facebook</code></td>
<td>Displays guest users using Facebook to log in</td>
</tr>
<tr>
<td><code>rfdomain &lt;DOMAIN-NAME&gt;</code></td>
<td>Displays guest users for a specific RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</td>
</tr>
<tr>
<td><code>wlan &lt;WLAN-NAME&gt;</code></td>
<td>Displays guest users for a specific WLAN</td>
</tr>
<tr>
<td></td>
<td>• &lt;WLAN-NAME&gt; – Specify the WLAN name.</td>
</tr>
<tr>
<td><code>google</code></td>
<td>Displays guest users using Google to log in</td>
</tr>
</tbody>
</table>
### Examples

nx9500-6C8809# show guest-registration **age-range** time all  
**Timeline:** all  

<table>
<thead>
<tr>
<th>AGE RANGE</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>less_than_18</td>
<td>0 ( 0%)</td>
</tr>
<tr>
<td>18_to_24</td>
<td>1 ( 20%)</td>
</tr>
<tr>
<td>25_to_34</td>
<td>0 ( 0%)</td>
</tr>
<tr>
<td>35_to_44</td>
<td>1 ( 20%)</td>
</tr>
<tr>
<td>45_to_54</td>
<td>1 ( 20%)</td>
</tr>
<tr>
<td>55_to_64</td>
<td>2 ( 40%)</td>
</tr>
<tr>
<td>greater_than_64</td>
<td>0 ( 0%)</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809# show guest-registration **browsers** time 1-Day rfdomain Test-rfdomain-10  
**RF Domain:** Test-rfdomain-10 **Timeline:** 1-Day  

<table>
<thead>
<tr>
<th>BROWSER</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safari</td>
<td>1 ( 50%)</td>
</tr>
<tr>
<td>Chrome</td>
<td>1 ( 50%)</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809# show guest-registration **devices** time 30-Mins wlan Test-ssid-9  
**WLAN:** Test-ssid-9 **Timeline:** 30-Mins  

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows PC</td>
<td>1 (100%)</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809# show guest-registration **gender** time all wlan Test-ssid-10 rfdomain Test-rfdomain-10  
**RF Domain:** Test-rfdomain-10 **WLAN:** Test-ssid-10 **Timeline:** all  

<table>
<thead>
<tr>
<th>GENDER</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>1 ( 50%)</td>
</tr>
<tr>
<td>Female</td>
<td>1 ( 50%)</td>
</tr>
<tr>
<td>Other</td>
<td>0 ( 0%)</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809# show guest-registration **gender** time all wlan Test-ssid-10 rfdomain Test-rfdomain-9  
%% No guests registered for specified inputs.  

nx9500-6C8809#

nx9500-6C8809# show guest-registration **os** time 1-Day  
**Timeline:** 1-Day  

<table>
<thead>
<tr>
<th>OS</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>3 ( 30%)</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>3 ( 30%)</td>
</tr>
<tr>
<td>Macintosh</td>
<td>3 ( 30%)</td>
</tr>
<tr>
<td>Windows 8</td>
<td>1 ( 10%)</td>
</tr>
</tbody>
</table>
nx9500-6C8809#show guest-registration social time 30-Mins

**Timeline: 30-Mins**

<table>
<thead>
<tr>
<th>SOCIAL</th>
<th>ONLINE</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>google</td>
<td>1 (100%)</td>
<td>1 (10%)</td>
</tr>
<tr>
<td>Local</td>
<td>0 (0%)</td>
<td>9 (90%)</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809#show guest-registration user-trends time all

**Timeline: all**

<table>
<thead>
<tr>
<th>SAMPLE RANGE</th>
<th>NEW USERS</th>
<th>RETURN USERS</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-2-16 - 2014-4-17</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>2014-4-17 - 2014-6-16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>2014-6-16 - 2014-8-15</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>2014-8-15 - 2014-10-14</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>2014-10-14 - 2014-12-13</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>2014-12-13 - 2015-2-11</td>
<td>10 (100%)</td>
<td>0 (0%)</td>
<td>10</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809#show guest-registration user-trends time 1-Day

**Timeline: 1-Day**

<table>
<thead>
<tr>
<th>SAMPLE RANGE</th>
<th>NEW USERS</th>
<th>RETURN USERS</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>23:16 - 3:16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>3:16 - 7:16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>7:16 - 11:16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>11:16 - 15:16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>15:16 - 19:16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
<tr>
<td>19:16 - 23:16</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809#show guest-registration visitors time 30-Mins

**Timeline: 30-Mins**

<table>
<thead>
<tr>
<th>VISITORS</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Users</td>
<td>7 (70%)</td>
</tr>
<tr>
<td>Return Users</td>
<td>3 (30%)</td>
</tr>
</tbody>
</table>

nx9500-6C8809#
nx9500-6C8809#show guest-registration client time 30-Mins email Guest_9@abc.com

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>city</td>
<td>Brooklyn</td>
</tr>
<tr>
<td>wlan</td>
<td>Test-ssid-10</td>
</tr>
<tr>
<td>name</td>
<td>Guest_9</td>
</tr>
<tr>
<td>zip</td>
<td>11204</td>
</tr>
<tr>
<td>mobile</td>
<td>9131373709</td>
</tr>
<tr>
<td>gender</td>
<td>female</td>
</tr>
<tr>
<td>llogintime</td>
<td>2015-01-20 19:11:14.001000</td>
</tr>
<tr>
<td>mobileok</td>
<td>on</td>
</tr>
<tr>
<td>devtype</td>
<td>Windows PC</td>
</tr>
<tr>
<td>createtime</td>
<td>2015-01-20 18:27:14.001000</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:Guest_9@abc.com">Guest_9@abc.com</a></td>
</tr>
<tr>
<td>mac</td>
<td>10-00-00-10-00-09</td>
</tr>
<tr>
<td>reg_type</td>
<td>otp</td>
</tr>
<tr>
<td>rfd</td>
<td>Test-rfdomain-10</td>
</tr>
<tr>
<td>agerange</td>
<td>&lt;18</td>
</tr>
<tr>
<td>group</td>
<td>mac_reg_gr1</td>
</tr>
<tr>
<td>mid</td>
<td>1234100009</td>
</tr>
<tr>
<td>os</td>
<td>Windows 7</td>
</tr>
<tr>
<td>browser</td>
<td>Safari</td>
</tr>
</tbody>
</table>

nx9500-6C8809#

nx9500-6C8809#show guest-registration client time 30-Mins rfdomain Test-rfdomain-8

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>loggedin</td>
<td>yes</td>
</tr>
<tr>
<td>wlan</td>
<td>Test-ssid-8</td>
</tr>
<tr>
<td>name</td>
<td>Guest_1</td>
</tr>
<tr>
<td>locale</td>
<td>en_US</td>
</tr>
<tr>
<td>llogintime</td>
<td>2015-01-20 19:15:14</td>
</tr>
<tr>
<td>devtype</td>
<td>Macintosh</td>
</tr>
<tr>
<td>exptime</td>
<td>2015-11-16 19:21:14</td>
</tr>
<tr>
<td>lname</td>
<td>Guest_100000</td>
</tr>
<tr>
<td>source</td>
<td>google</td>
</tr>
<tr>
<td>mac</td>
<td>10-00-00-10-00-01</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:Guest_1@abc.com">Guest_1@abc.com</a></td>
</tr>
<tr>
<td>id</td>
<td>657669862939196</td>
</tr>
<tr>
<td>reg_type</td>
<td>device</td>
</tr>
<tr>
<td>fname</td>
<td>Test-Guest_1</td>
</tr>
<tr>
<td>rfd</td>
<td>Test-rfdomain-8</td>
</tr>
<tr>
<td>agerange</td>
<td>35-44</td>
</tr>
<tr>
<td>timezone</td>
<td>7</td>
</tr>
<tr>
<td>profilePic</td>
<td><a href="https://www.google.com/user_id/657669862939196/">https://www.google.com/user_id/657669862939196/</a></td>
</tr>
<tr>
<td>os</td>
<td>Macintosh</td>
</tr>
<tr>
<td>createtime</td>
<td>2015-01-20 18:45:14</td>
</tr>
<tr>
<td>group</td>
<td>mac_reg_gr1</td>
</tr>
<tr>
<td>browser</td>
<td>Chrome</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>city</td>
<td>Santa Cruz</td>
</tr>
<tr>
<td>group</td>
<td>mac_reg_gr1</td>
</tr>
<tr>
<td>name</td>
<td>Guest_2</td>
</tr>
<tr>
<td>zip</td>
<td>95062</td>
</tr>
<tr>
<td>mobile</td>
<td>3700870747</td>
</tr>
<tr>
<td>mid</td>
<td>1234100001</td>
</tr>
<tr>
<td>llogintime</td>
<td>2015-01-20 19:18:14</td>
</tr>
<tr>
<td>mobileok</td>
<td>on</td>
</tr>
<tr>
<td>devtype</td>
<td>Apple iPad</td>
</tr>
<tr>
<td>exptime</td>
<td>2015-11-16 19:21:14</td>
</tr>
<tr>
<td>createtime</td>
<td>2015-01-20 19:11:14</td>
</tr>
<tr>
<td>mac</td>
<td>10-00-00-10-00-02</td>
</tr>
<tr>
<td>reg_type</td>
<td>otp</td>
</tr>
<tr>
<td>rfd</td>
<td>Test-rfdomain-8</td>
</tr>
</tbody>
</table>
agerange       55-64
wlan           Test-ssid-8
os             Apple iOS
email          Guest_2@abc.com
browser        Chrome
-----------------------------------
city           Los Angeles
group          mac_reg_gr1
name           Guest_5
zip            90001
mobile         9129618672
mid            1234100005
llogintime     2015-01-20 19:20:14
devtype        Macintosh
exptime        2015-11-16 19:21:14
createtime     2015-01-20 19:05:14
mac            10-00-00-10-00-05
reg_type       device
rfd            Test-rfdomain-8
agerange       18-24
wlan           Test-ssid-8
os             Macintosh
email          Guest_5@abc.com
browser        Chrome
-----------------------------------
nx9500-6C8809#
### 6.1.31 interface

#### show commands
Displays configured system interfaces and their status

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
show interface {<INTERFACE-NAME>|brief|counters|ge|me1|port-channel|pppoe1|
switchport|vlan|wwan1} {on <DEVICE-NAME>}
show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|port-channel <1-2>|
pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}
```

#### Parameters
- `<INTERFACE-NAME>`
  - Optional. Displays the interface specified by the `<INTERFACE-NAME>` parameter. Specify the interface name.
- `brief`
  - Optional. Displays a brief summary of the interface status and configuration
- `counters`
  - Optional. Displays interface Tx or Rx counters
- `ge <1-4>`
  - Optional. Displays Gigabit Ethernet interface status and configuration
    - `<1-4>` – Select the Gigabit Ethernet interface index from 1 - 4.
    - **Note:** For the NX45XX and NX65XX service platforms the index range is <1 - 24>.
- `me1`
  - Optional. Displays Fast Ethernet interface status and configuration
- `port-channel <1-2>`
  - Optional. Displays port channel interface status and configuration
    - `<1-2>` – Specify the port channel index from 1 - 2.
- `pppoe1`
  - Optional. Displays PPP over Ethernet interface status and configuration
- `switchport`
  - Optional. Displays layer 2 interface status
- `vlan <1-4094>`
  - Optional. Displays VLAN interface status and configuration
    - `<1-4094>` – Specify the Switch Virtual Interface (SVI) VLAN ID from 1 - 4094.
- `wwan1`
  - Optional. Displays Wireless WAN interface status, configuration, and counters
- `on <DEVICE-NAME>`
  - The following keywords are common to all of the above interfaces:
    - `on <DEVICE-NAME>` – Optional. Displays interface related information on a specified device
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.
Examples

Following interfaces are available on a RFS7000 controller:

```
rfs7000-6DCD4B(config)#show interface ?
WORD          Interface name
brief         Brief summary of interface status and configuration
counters      Interface tx/rx counters
ge            GigabitEthernet interface
me1           FastEthernet interface
on            On AP/Controller
port-channel  Port-Channel interface
pppoe1        PPP Over Ethernet interface
switchport    Status of Layer2 interfaces
vlan          Switch VLAN interface
wwan1         Wireless WAN interface
|             Output modifiers
>             Output redirection
>>            Output redirection appending
<cr>
```

 Following interfaces are available on a NX45XX and NX65XX series service platform:

```
nx4500-5CFA2B(config)#show interface ?
WORD        Interface name
brief       Brief summary of interface status and configuration
counters    Interface tx/rx counters
ge          GigabitEthernet interface
on          On AP/Controller
pppoe1      PPP Over Ethernet interface
serial      Serial interface
switchport  Status of Layer2 interfaces
t1e1        T1/E1 interface
up          WAN Ethernet interface
vlan        Switch VLAN interface
vmif        Virtual Machine interface
wwan1       Wireless WAN interface
|           Output modifiers
>           Output redirection
>>          Output redirection appending
<cr>
```

rfs7000-6DCD4B(config)#show interface switchport

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>STATUS</th>
<th>MODE</th>
<th>VLAN(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge1</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>ge2</td>
<td>UP</td>
<td>access</td>
<td>192</td>
</tr>
<tr>
<td>ge3</td>
<td>DOWN</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>ge4</td>
<td>DOWN</td>
<td>access</td>
<td>1</td>
</tr>
</tbody>
</table>

A '*' next to the VLAN ID indicates the native vlan for that trunk port

```
rfs7000-6DCD4B(config)#
```

rfs7000-6DCD4B(config)#show interface ge 2
Interface ge2 is UP
Hardware-type: ethernet, Mode: Layer 2, Address: B4-C7-99-6D-CD-4D
Index: 2002, Metric: 1, MTU: 1500
Speed: Admin Auto, Operational 100M, Maximum 1G
Duplex: Admin Auto, Operational Full
Active-medium: Copper
Switchport settings: access, access-vlan: 192
Input packets 356055, bytes 118606892, dropped 0
Received 55855 unicasts, 38581 broadcasts, 261619 multicasts
Input errors 0, runts 0, giants 0
CRC 0, frame 0, fragment 0, jabber 0
Output packets 24790, bytes 2250297, dropped 0
Sent 21651 unicasts, 4 broadcasts, 3135 multicasts
Output errors 0, collisions 0, late collisions 0
Excessive collisions 0

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show interface counters

<table>
<thead>
<tr>
<th>INTF</th>
<th>MAC</th>
<th>RX-PKTS</th>
<th>RX-BYTES</th>
<th>RX-DROP</th>
<th>TX-PKTS</th>
<th>TX-BYTES</th>
<th>TX-DROP</th>
</tr>
</thead>
<tbody>
<tr>
<td>me1</td>
<td>B4-C7-99-6D-CD-50</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan1</td>
<td>B4-C7-99-6D-CD-4B</td>
<td>302809</td>
<td>31378711</td>
<td>0</td>
<td>287885</td>
<td>31198711</td>
<td>0</td>
</tr>
<tr>
<td>vlan192</td>
<td>B4-C7-99-6D-CD-4B</td>
<td>348726</td>
<td>109702923</td>
<td>0</td>
<td>72561</td>
<td>77318385</td>
<td>0</td>
</tr>
<tr>
<td>ge1</td>
<td>B4-C7-99-6D-CD-4C</td>
<td>135448</td>
<td>18211575</td>
<td>0</td>
<td>196016</td>
<td>23063136</td>
<td>0</td>
</tr>
<tr>
<td>ge2</td>
<td>B4-C7-99-6D-CD-4D</td>
<td>353593</td>
<td>118284345</td>
<td>0</td>
<td>24517</td>
<td>2213093</td>
<td>0</td>
</tr>
<tr>
<td>ge3</td>
<td>B4-C7-99-6D-CD-4E</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>37316</td>
<td>3552250</td>
<td>0</td>
</tr>
<tr>
<td>ge4</td>
<td>B4-C7-99-6D-CD-4F</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>37316</td>
<td>3552250</td>
<td>0</td>
</tr>
</tbody>
</table>

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show interface vlan 1

Interface vlan1 is UP
Hardware-type: vlan, Mode: Layer 3, Address: B4-C7-99-6D-CD-4B
Index: 27, Metric: 1, MTU: 1500
IP-Address: 192.168.13.12/24
input packets 503614, bytes 610738458, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 503614, bytes 610738458, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
IPv6 mode is disabled

nx4500-5CFA2B(config)#

nx4500-5CFA2B(config)#show interface switchport

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>STATUS</th>
<th>MODE</th>
<th>VLAN(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>up1</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>up2</td>
<td>DOWN</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif1</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif2</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif3</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif4</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif5</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif6</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif7</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
<tr>
<td>vmif8</td>
<td>UP</td>
<td>access</td>
<td>1</td>
</tr>
</tbody>
</table>

A '*' next to the VLAN ID indicates the native vlan for that trunk port

nx4500-5CFA2B(config)#

nx4500-5CFA2B(config)#show interface vlan 1

Interface vlan1 is UP
Hardware-type: vlan, Mode: Layer 3, Address: B4-C7-99-5C-FA-2B
Index: 27, Metric: 1, MTU: 1500
IP-Address: 192.168.13.12/24
input packets 1664443, bytes 198932875, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 903614, bytes 110738458, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
IPv6 mode is disabled

nx4500-5CFA2B(config)#
nx4500-5CFA2B(config)#show interface ge 2
Interface ge2 is DOWN
Hardware-type: ethernet, Mode: Layer 2, Address: B4-C7-99-5C-FA-2B
Index: 2002, Metric: 1, MTU: 1500
Speed: Admin Auto, Operational n/a, Maximum 1G
Duplex: Admin Auto, Operational n/a
Active-medium: n/a
Switchport settings: access, access-vlan: 1
Input packets 0, bytes 0, dropped 0
Received 0 unicast, 0 broadcasts, 0 multicasts
Input errors 0, runts 0, giants 0
CRC 0, frame 0, fragment 0, jabber 0
Output packets 501587, bytes 60935912, dropped 0
Sent 3 unicast, 4613 broadcast, 496971 multicast
Output errors 0, collisions 0, late collisions 0
Excessive collisions 0

nx4500-5CFA2B(config)#

nx4500-5CFA8E(config)#show interface counters
---------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>INTF</th>
<th>MAC</th>
<th>RX-PKTS</th>
<th>RX-BYTES</th>
<th>RX-DROP</th>
<th>TX-PKTS</th>
<th>TX-BYTES</th>
<th>TX-DROP</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1</td>
<td>B4-C7-99-5C-FA-8E</td>
<td>976838</td>
<td>104430807</td>
<td>0</td>
<td>3320</td>
<td>105117</td>
<td>0</td>
</tr>
<tr>
<td>up1</td>
<td>B4-C7-99-5C-FA-8F</td>
<td>1000205</td>
<td>121668156</td>
<td>0</td>
<td>768931</td>
<td>77779941</td>
<td>0</td>
</tr>
<tr>
<td>up2</td>
<td>B4-C7-99-5C-FA-90</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vmif1</td>
<td>02-16-3E-05-00-01</td>
<td>279901</td>
<td>32766488</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vmif2</td>
<td>02-16-3E-05-00-02</td>
<td>279901</td>
<td>32766488</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vmif3</td>
<td>02-16-3E-05-00-03</td>
<td>279901</td>
<td>32766488</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vmif4</td>
<td>02-16-3E-05-00-04</td>
<td>279901</td>
<td>32766488</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vmif5</td>
<td>02-16-3E-05-00-05</td>
<td>279901</td>
<td>32766488</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>--More--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

nx4500-5CFA8E(config)#
6.1.32 ip

show commands

Displays IP related information

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show ip [arp|bgp|ddns|default-gateways|dhcp|dhcp-vendor-options|domain-name|
    extcommunity-list|igmp|interface|name-server|nat|ospf|route|routing]

show ip arp {<VLAN-NAME>} {on <DEVICE-NAME>}

show ip bgp {<IP>|<IP/M>|community|community-list|filter-list|neighbors|on|paths|
    prefix-list|regexp|route-map|state|summary}

show ip ddns bindings {on <DEVICE-NAME>}

show ip dhcp [binding|networks|status]

show ip dhcp binding [manual] {on <DEVICE-NAME>}

show ip dhcp [networks|status] {on <DEVICE-NAME>}

show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing]
    {on <DEVICE-NAME>}

show ip extcommunity-list [1-500]|<NAME>]

show ip igmp snooping [mrouter|querier|vlan]

show ip igmp snooping [mrouter|querier] vlan <1-4095> {on <DEVICE-NAME>}

show ip interface {<INTERFACE-NAME>|brief|on}

show ip interface {<INTERFACE-NAME>|brief} {on <DEVICE-NAME>}

show ip nat translations verbose {on <DEVICE-NAME>}

show ip route {<INTERFACE-NAME>|ge|me1|on|port-channel|pppoel|vlan|wwan1}

show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|
    pppoe1|wwan1} {on <DEVICE-NAME>}

show ip ospf {border-router|interface|neighbor|on|route|state}

show ip ospf {border-router|neighbor|route|on|state} {on <DEVICE-NAME>}

show ip ospf [interface] {vlan|on}

show ip ospf [interface] {vlan <1-4094>} {on <DEVICE-NAME>}

---

**NOTE:** The show ip ospf command is also available under the 'profile' and 'device' modes.

### Parameters

- **show ip arp {<VLAN-NAME>}** {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp</td>
<td>Displays Address Resolution Protocol (ARP) mappings</td>
</tr>
<tr>
<td>&lt;VLAN-NAME&gt;</td>
<td>Optional. Displays ARP mapping on a specified VLAN. Specify the VLAN name.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'vlan-name' parameter:  
  - on <DEVICE-NAME> – Optional. Displays ARP configuration details on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| ip bgp        | Displays BGP routing table statistics based on the match criteria specified here. Routes matching the specified criteria are filtered. Use available options to filter the information displayed.  
  **Note:** This command is applicable to the RFS4000, RFS6000, NX45XX, NX65XX, NX9XXX model devices. |
| <IP>          | Optional. Filters routes matching the specified IP address                                              |
| <IP/M>        | Optional. Filters routes matching the specified network                                               |
| community     | Optional. Filters routes based on the community attribute specified. The options are:  
  - AA:NN – Filters routes based on the community number (AA: is the autonomous system number (ASN), NN: is the community number within the specified ASN)  
  - local-as – Filters routes carrying the local-as attribute (these routes are not sent outside the local AS)  
  - no-advertise – Filters routes carrying the no-advertise attribute (these routes are not advertised to any peers)  
  - no-export – Filters routes carrying no-export attribute (these routes are not exported to next AS) |
| community-list| Optional. Displays routes that are members of communities included in the specified BGP community-list  
  - <1-500> – Specify the community-list number.  
  - <WORD> – Specify the community-list name. |
| filter-list   | Optional. Filters routes having AS-path matching the specified AS-path access list. Specify the AS-path ACL name. |
| neighbors     | Optional. Displays BGP neighbor details. Specify the IP address, to view a specific neighbor details. Use one of the following options to filter information:  
  - advertised-routes – Displays route information for routes advertised to the selected neighbor device  
  - received-routes – Displays route information for routes received from the selected neighbor device  
  - routes – Displays the route information for routes learned from the selected neighbor device  
  **Note:** If no neighbor IP address is specified, the system displays all neighbor-related routes on the logged device. |
| on <DEVICE-NAME> | Optional. Displays BGP routing table statistics on a specified device  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
<p>| paths         | Optional. Displays BGP path details                                                                       |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip ddns bindings</strong> <em>(on &lt;DEVICE-NAME&gt;)</em></td>
<td>Displays Dynamic Domain Name Server (DDNS) configuration details.</td>
</tr>
<tr>
<td><em>ip ddns</em></td>
<td>Displays DDNS address bindings.</td>
</tr>
<tr>
<td><em>bindings</em> <em>(on &lt;DEVICE-NAME&gt;)</em></td>
<td>Displays DDNS address bindings.</td>
</tr>
<tr>
<td><em>regexp &lt;LINE&gt;</em></td>
<td>Displays routes matching the specified AS path regular expression.</td>
</tr>
<tr>
<td><em>route-map &lt;ROUTE-MAP-NAME&gt;</em>**</td>
<td>Displays routes matching the specified route map.</td>
</tr>
<tr>
<td><em>prefix-list &lt;PREFIX-LIST-NAME&gt;</em></td>
<td>Displays routes confirming to the specified prefix-list.</td>
</tr>
<tr>
<td><em>regexp &lt;LINE&gt;</em></td>
<td>Displays routes matching the specified AS path regular expression.</td>
</tr>
<tr>
<td><em>route-map &lt;ROUTE-MAP-NAME&gt;</em></td>
<td>Displays routes matching the specified route map.</td>
</tr>
</tbody>
</table>

**Note:**
- This command is applicable to the RFS4000, RFS6000, NX45XX, NX65XX, NX9XXX model devices.
### SHOW COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip default-gateways</code></td>
<td>Displays all learnt default gateways</td>
</tr>
<tr>
<td><code>show ip dhcp-vendor-options</code></td>
<td>Displays DHCP 43 parameters received from the DHCP server. This output includes the interface from which the option was learned.</td>
</tr>
<tr>
<td><code>show ip domain-name</code></td>
<td>Displays the DNS default domain</td>
</tr>
<tr>
<td><code>show ip name-server</code></td>
<td>Displays the DNS name server details</td>
</tr>
<tr>
<td><code>show ip routing</code></td>
<td>Displays routing status</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keywords are common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays IP related information, based on the parameters passed, on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp snooping mrouter</code></td>
<td>Displays the IGMP snooping configuration</td>
</tr>
<tr>
<td><code>show ip igmp snooping querier</code></td>
<td>Displays the IGMP snooping multicast querier configuration</td>
</tr>
<tr>
<td><code>show ip igmp snooping vlan &lt;1-4095&gt;</code></td>
<td>Displays the IGMP snooping multicast router (mrouter) configuration for a VLAN</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4095&gt; – Specify the VLAN ID from 1 - 4095.</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays the IGMP snooping mrouter configuration on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP or wireless controller.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp snooping vlan &lt;1-4095&gt; {&lt;IP&gt;} {on &lt;DEVICE-NAME&gt;}</code></td>
<td>Displays the VLAN IGMP snooping configuration</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4095&gt; – Specify the VLAN ID from 1 - 4095.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP&gt; – Optional. Specifies the multicast group IP address</td>
</tr>
<tr>
<td></td>
<td>on &lt;DEVICE-NAME&gt; – The following keyword is recursive and common to the 'ip' parameter:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays configuration details on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP or wireless controller.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip interface</code></td>
<td>Displays an administrative and operational status of all layer 3 interfaces or a specified layer 3 interface</td>
</tr>
<tr>
<td><code>&lt;INTERFACE-NAME&gt;</code></td>
<td>Optional. Displays a specified interface status. Specify the interface name.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><code>show ip route</code></td>
<td>Displays route table details. The route tables use flags to distinguish between routes. The different flags are: C – Connected, G – Gateway, O – OSPF route, S – Static route. Note: Flags ‘S’ and ‘O’ identify static learned routes and dynamic learned routes respectively.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>Optional. Displays a brief summary of all interface status and configuration.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keyword is recursive and common to the ‘interface-name’ and ‘brief’ parameters: on &lt;DEVICE-NAME&gt; – Optional. Displays interface status and summary, based on the parameters passed, on a specified device. &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><code>ip ospf</code></td>
<td>Displays overall OSPF information.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keywords are recursive and common to all of the above parameters: on &lt;DEVICE-NAME&gt; – Displays route table details, based on the parameters passed, on a specified device. &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Example Commands:**

- `show ip nat translations verbose {on <DEVICE-NAME>}`
- `show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|pppoe1|wwan1} {on <DEVICE-NAME>}`
- `show ip ospf {border-router|interface|neighbor|route|on|state} {on <DEVICE-NAME>}`
### Examples

rfs7000-6DCD4B(config)# show ip arp
```
<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>INTERFACE</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.18.0.1</td>
<td>00-23-68-22-9D-58</td>
<td>vlan1</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.13.10</td>
<td>00-02-B3-28-D1-55</td>
<td>vlan192</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.13.2</td>
<td>00-0F-8F-19-BA-4C</td>
<td>vlan192</td>
<td>dynamic</td>
</tr>
</tbody>
</table>
```

rfs7000-6DCD4B(config)# show ip interface brief
```
<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>IP-ADDRESS/MASK</th>
<th>TYPE</th>
<th>STATUS</th>
<th>PROTOCOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>me1</td>
<td>192.168.0.1/24</td>
<td>primary</td>
<td>UP</td>
<td>down</td>
</tr>
<tr>
<td>vlan1</td>
<td>172.168.0.2/24</td>
<td>primary</td>
<td>UP</td>
<td>up</td>
</tr>
<tr>
<td>vlan192</td>
<td>192.168.13.111/24</td>
<td>primary</td>
<td>UP</td>
<td>up</td>
</tr>
</tbody>
</table>
```

rfs7000-6DCD4B(config)# show ip route test
```
+---------------------------------+-----------------+--------+------------+----------|
<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>157.235.208.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan4</td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
<tr>
<td>default</td>
<td>172.16.10.9</td>
<td>CG</td>
<td>vlan1</td>
</tr>
</tbody>
</table>
```

Flags:  
- C - Connected  
- G - Gateway
rfs7000-6DCD4B(config)#show ip route port-channel 1

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/24</td>
<td>direct</td>
<td>C</td>
<td>me1</td>
</tr>
<tr>
<td>172.18.0.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
<tr>
<td>10.2.0.0/24</td>
<td>172.18.0.1</td>
<td>S</td>
<td>vlan1</td>
</tr>
<tr>
<td>default</td>
<td>192.168.13.2</td>
<td>S</td>
<td>vlan192</td>
</tr>
<tr>
<td>192.168.13.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan192</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway  O - OSPF  B - BGP  S - Static
Gateway:  N - Normalized Gateway Address

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show ip route vlan 1

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.18.0.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
<tr>
<td>10.2.0.0/24</td>
<td>172.18.0.1</td>
<td>S</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway  O - OSPF  B - BGP  S - Static
Gateway:  N - Normalized Gateway Address

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show ip route ge 1

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/24</td>
<td>direct</td>
<td>C</td>
<td>me1</td>
</tr>
<tr>
<td>172.18.0.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
<tr>
<td>10.2.0.0/24</td>
<td>172.18.0.1</td>
<td>S</td>
<td>vlan1</td>
</tr>
<tr>
<td>default</td>
<td>192.168.13.2</td>
<td>S</td>
<td>vlan192</td>
</tr>
<tr>
<td>192.168.13.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan192</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway  O - OSPF  B - BGP  S - Static
Gateway:  N - Normalized Gateway Address

rfs7000-6DCD4B(config)#

rfs7000-6DCD4B(config)#show ip routing on rfs6000-81742D
IP routing is enabled.

rfs7000-6DCD4B(config)#

rfs7000-37FABE(config)#show ip dhcp status
State of DHCP server: running
Interfaces: vlan2, vlan3

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip ospf state
Maximum number of OSPF routes allowed: 9216
  Number of OSPF routes received: 0
  Ignore-count allowed: 5, current ignore-count: 0
  Ignore-time 60 seconds, reset-time 360 seconds
  Current OSPF process state: Running

rfs7000-37FABE(config)#
rfs7000-37FABE#show ip route vlan 1

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway  O - OSPF  S - Static

rfs4000-882A17#show ip route on ap7131-0B863C

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.9.0/24</td>
<td>192.168.0.12</td>
<td>O</td>
<td>vlan10</td>
</tr>
<tr>
<td>192.168.5.0/24</td>
<td>192.168.0.12</td>
<td>O</td>
<td>vlan10</td>
</tr>
<tr>
<td>192.168.6.0/24</td>
<td>192.168.0.12</td>
<td>O</td>
<td>vlan10</td>
</tr>
<tr>
<td>172.20.15.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan66</td>
</tr>
<tr>
<td>99.99.99.96/32</td>
<td>192.168.0.53</td>
<td>S</td>
<td>vlan10</td>
</tr>
<tr>
<td>99.99.99.97/32</td>
<td>192.168.0.40</td>
<td>S</td>
<td>vlan10</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway  O - OSPF  S - Static

nx6500-31FABE(config)#show ip route ge 1

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.12.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan3</td>
</tr>
<tr>
<td>172.16.11.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan2</td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway

nx6500-31FABE(config)#show ip routing
IP routing is enabled.

nx6500-31FABE(config)#show ip dhcp status
State of DHCP server: running
Interfaces: vlan2, vlan3

nx6500-31FABE(config)#

rfs4000-229D58#show ip dhcp-vendor-options

<table>
<thead>
<tr>
<th>ITEM</th>
<th>VALUE</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Info</td>
<td>n/a</td>
<td>vlan400</td>
</tr>
<tr>
<td>Firmware Image File</td>
<td>n/a</td>
<td>vlan400</td>
</tr>
<tr>
<td>Config File</td>
<td>n/a</td>
<td>vlan400</td>
</tr>
<tr>
<td>Legacy Adoption Info</td>
<td>192.168.30.1</td>
<td>vlan300</td>
</tr>
<tr>
<td>AP Adoption Info</td>
<td>192.168.50.2</td>
<td>vlan500</td>
</tr>
<tr>
<td>AP Adoption Info</td>
<td>192.168.50.3</td>
<td>vlan500</td>
</tr>
<tr>
<td>Controller Adoption Info</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

rfs4000-229D58#
### 6.1.33 ip-access-list

**show commands**

Displays IP access list statistics

---

**NOTE:** This command is not available in the USER EXEC Mode.

---

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail|on}
show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail <IP-ACCESS-LIST-NAME>}
{(on <DEVICE-NAME>)}
```

**Parameters**

- `show ip-access-list stats {<IP-ACCESS-LIST-NAME>|detail|on}`
- `{<IP-ACCESS-LIST-NAME>|detail <IP-ACCESS-LIST-NAME>}`
- `(on <DEVICE-NAME>)`

- **ip-access-list stats**
  - Displays IP access list statistics

- **<IP-ACCESS-LIST-NAME>**
  - Optional. Displays statistics for a specified IP access list. Specify the IP access list name.

- **detail**
  - `<IP-ACCESS-LIST-NAME>`
  - Optional. Displays detailed statistics for a specified IP access list. Specify the IP access list name.

- **on <DEVICE-NAME>**
  - The following keyword is recursive and common to the 'IP-ACCESS-LIST-NAME' and 'detail' parameters:
    - `on <DEVICE-NAME>` – Optional. Displays all or a specified IP access list statistics on a specified device.
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

**Examples**

```
rfs7000-37FABE(config)#show ip-access-list stats
IP Access-list: # Restrict Management ACL #
   permit tcp any any eq ftp rule-precedence 1       Hitcount: 0
   permit tcp any any eq www rule-precedence 2       Hitcount: 4
   permit tcp any any eq ssh rule-precedence 3       Hitcount: 448
   permit tcp any any eq https rule-precedence 4      Hitcount: 0
   permit udp any any eq snmp rule-precedence 5       Hitcount: 0
   permit tcp any any eq telnet rule-precedence 6      Hitcount: 4
rfs7000-37FABE(config)#
```
The following example displays the 'auto-tunnel-acl' IP ACL configuration:

```
rfs4000-229D58(config)#ip access-list auto-tunnel-acl
rfs4000-229D58(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
permit ip host 200.200.200.99 any rule-precedence 3
rfs4000-229D58(config-ip-acl-auto-tunnel-acl)#
```

The following example displays the statistics for the 'auto-tunnel-acl' ACL:

```
rfs4000-229D58#show ip-access-list stats
IP Access-list: auto-tunnel-acl
permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2 Hitcount: 0
permit ip host 200.200.200.99 any rule-precedence 3 Hitcount: 0
rfs4000-229D58#
```

```
x6524-5483B0#show ip-access-list stats scaleacl | i 125
Hitcount: 893 Hardware
Hitcount: 3120
permit ip host 125.1.1.1 any rule-precedence 125 Hitcount: 0
permit ip host 125.2.1.1 any rule-precedence 346 Hitcount: 0
x6524-5483B0#
```
### 6.1.34 ipv6

> **show commands**

Displays IPv6 related information

**Supported in the following platforms:**

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show ipv6 [default-gateways|delegated-prefix|dhcp|hop-limit|interface|mld|name-server|neighbors|route]
show ipv6 [default-gateways|delegated-prefix|hop-limit|name-server] {on <DEVICE-NAME>}
show ipv6 dhcp [client received-options|relay status|status] {on <DEVICE-NAME>}
show ipv6 interface {<IF-NAME>|brief} {on <DEVICE-NAME>}
show ipv6 mld snooping [mrouter vlan <1-4095>|querier vlan <1-4095>|vlan <1-4095>] {on <DEVICE-NAME>}
show ipv6 neighbors <VLAN-NAME> {on <DEVICE-NAME>}
show ipv6 route {<IF-NAME>|ge <1-X>|me1|port-channel <1-2>|pppoe1|serial <1-4>|t1e1 <1-4> |<1-4> |up|vlan <1-4095>|vmif <1-X>|wwan1|xge} {on <DEVICE-NAME>}
```

**Parameters**

- `ipv6` Displays IPv6 related information
- `default-gateways` Displays all learnt default gateways
- `delegated-prefix` Displays prefix delegation information
- `hop-limit` Displays the configured IPv6 hop count value
- `name-server` Displays DNS name servers
- `on <DEVICE-NAME>` This parameter is common to all of the above keywords.
  - `on <DEVICE-NAME>` – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

- `show ipv6 dhcp [client received-options|relay status|status] {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Displays IPv6 related information</td>
</tr>
<tr>
<td>default-gateways</td>
<td>Displays all learnt default gateways</td>
</tr>
<tr>
<td>delegated-prefix</td>
<td>Displays prefix delegation information</td>
</tr>
<tr>
<td>hop-limit</td>
<td>Displays the configured IPv6 hop count value</td>
</tr>
<tr>
<td>name-server</td>
<td>Displays DNS name servers</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>This parameter is common to all of the above keywords.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Displays DHCPv6 related information</td>
</tr>
<tr>
<td>client received-options</td>
<td>Displays DHCP options received from clients</td>
</tr>
<tr>
<td>relay status</td>
<td>Displays the DHCPv6 relay agent’s running status</td>
</tr>
</tbody>
</table>
### SHOW COMMANDS 6-83

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Displays the DHCPv6 stateless server daemon’s status. In case the DHCPv6 server is up and running, it also displays interface names.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>This parameter is common to all of the above keywords.</td>
</tr>
<tr>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

- **show ipv6 interface** `{<IF-NAME>|brief} {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Displays IPv6 related information</td>
</tr>
<tr>
<td>interface `{&lt;IF-NAME&gt;</td>
<td>brief}`</td>
</tr>
<tr>
<td>• &lt;IF-NAME&gt; – Optional. Specify the interface name.</td>
<td></td>
</tr>
<tr>
<td>• brief – Optional. Displays a brief summary of IPv6 status and configuration on the specified interface</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>This parameter is common to all of the above keywords.</td>
</tr>
<tr>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

- **show ipv6 mld snooping** `{mrouter vlan <1-4095>|querier vlan <1-4095>|vlan <1-4095}> {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Displays IPv6 related information</td>
</tr>
<tr>
<td>mld snooping</td>
<td>Displays Multicast Listener Discovery Protocol (MLD) snooping related information</td>
</tr>
<tr>
<td>mrouter vlan &lt;1-4095&gt;</td>
<td>Displays IPv6 multicast router information on the specified VLAN</td>
</tr>
<tr>
<td>querier vlan &lt;1-4095&gt;</td>
<td>Displays IPv6 multicast querier information on the specified VLAN</td>
</tr>
<tr>
<td>vlan &lt;1-4095&gt;</td>
<td>Displays MLD snooping related information on the specified VLAN</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>This parameter is common to all of the above keywords.</td>
</tr>
<tr>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

- **show ipv6 neighbors** `{<VLAN-NAME}> {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Displays IPv6 related information</td>
</tr>
<tr>
<td>neighbors <code>&lt;VLAN-NAME&gt;</code></td>
<td>Displays IPv6 neighbors on the specified VLAN</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays IPv6 neighbors on a specified device (access point, wireless controller, or service platform)</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>
**Examples**

```bash
rfs7000-37FABE(config)#show ipv6 dhcp client received-options
DHCPv6 Client received options:
  Interface: None
  Server Identifier: None
  Client Identifier: None
  DNS Servers: None
  Domain Name: None
  Sip Servers: None
  Sip Domain Name: None
  Refresh Time: None
```
Server Preference: 
  None
Vendor Options: 
  None

```
rfs7000-37FABE(config)#
```

```
rfs4000-229D58(config)# show ipv6 route
```

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:abcd::/64</td>
<td>fe80::300:1</td>
<td>S</td>
<td>vlan300</td>
</tr>
<tr>
<td>default</td>
<td>fe80::11:1</td>
<td>R</td>
<td>vlan11</td>
</tr>
<tr>
<td>4444:1111::/64</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Flags:  
C - Connected  
G - Gateway  
S - Static  
R - IPv6-RA

```
rfs4000-229D58(config)# show ipv6 default-gateways
```

<table>
<thead>
<tr>
<th>Source</th>
<th>Gateway-address</th>
<th>Preference</th>
<th>Status</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6-RA</td>
<td>fe80::100:1</td>
<td>medium</td>
<td>not-monitored</td>
<td>vlan100</td>
</tr>
<tr>
<td>low</td>
<td>Interface</td>
<td>NO</td>
<td>vlan1</td>
<td></td>
</tr>
<tr>
<td>medium</td>
<td>Remaining Lifetime: 1471 sec</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6-RA</td>
<td>fe80::11:1</td>
<td>low</td>
<td>not-monitored</td>
<td>vlan1</td>
</tr>
<tr>
<td>low</td>
<td>Interface</td>
<td>NO</td>
<td>vlan1</td>
<td></td>
</tr>
<tr>
<td>low</td>
<td>Remaining Lifetime: 1488 sec</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static-Route</td>
<td>fe80::2000:1</td>
<td>NA</td>
<td>unreachable</td>
<td>vlan2000</td>
</tr>
<tr>
<td>Preference</td>
<td>Status</td>
<td>Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static-Route</td>
<td>remaining Lifetime: forever</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6-RA</td>
<td>fe80::11:1</td>
<td>high</td>
<td>reachable</td>
<td>vlan11</td>
</tr>
<tr>
<td>Preference</td>
<td>Status</td>
<td>Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6-RA</td>
<td>fe80::11:1</td>
<td>high</td>
<td>reachable</td>
<td>vlan11</td>
</tr>
<tr>
<td>Preference</td>
<td>Status</td>
<td>Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
rfs4000-229D58#
```
6.1.35 ipv6-access-list

Display IPv6 access list statistics

NOTE: This command is not available in the USER EXEC Mode.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show ipv6-access-list stats <IPv6-ACCESS-LIST-NAME> {(on <DEVICE-NAME>)}

Parameters
- show ipv6-access-list stats <IPv6-ACCESS-LIST-NAME> {(on <DEVICE-NAME>)}

Examples
rfs6000-6DB5D4#show ipv6-access-list stats
IPV6 Access-list: test
deny ipv6 any any rule-precedence 20 Hitcount: 4
rfs6000-6DB5D4#
### 6.1.36 l2tpv3

**show commands**

Displays a Layer 2 Tunnel Protocol Version 3 (L2TPV3) session information

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
l2tpv3 {on|tunnel|tunnel-summary}
l2tpv3 {on <DEVICE-NAME>}
l2tpv3 {tunnel <L2TPV3-TUNNEL-NAME>} {session <L2TPV3-SESSION-NAME>}
{ (on <DEVICE-NAME>) }
l2tpv3 {tunnel-summary} { down|on|up }
l2tpv3 {tunnel-summary} { on <DEVICE-NAME> }
l2tpv3 {tunnel-summary} { down|up} { on <DEVICE-NAME> }
```

**Parameters**
- **l2tpv3 {on <DEVICE-NAME>}**

  Displays a L2TPv3 tunnel and session details or summary
  - on <DEVICE-NAME> – Optional. Displays L2TPv3 information on a specified access point or wireless controller
  - <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

- **l2tpv3 {tunnel <L2TPV3-TUNNEL-NAME>} {session <L2TPV3-SESSION-NAME>}**

  Optional. Displays a specified L2TPv3 tunnel information
  - <L2TPV3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name.

- **l2tpv3 {on <DEVICE-NAME>}**

  Optional. Displays a specified L2TPv3 tunnel session information
  - <L2TPV3-SESSION-NAME> – Specify the session name.

- **on <DEVICE-NAME>**

  The following keyword is recursive and common to the ‘session <L2TPV3-SESSION-NAME>’ parameter.
  - on <DEVICE-NAME> – Optional. Displays a L2TPv3 tunnel and session details, based on the parameters passed, on a specified device.
  - <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

**NOTE:** This command is not available in the USER EXEC mode.
l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}

- **l2tpv3**: Displays L2TPv3 tunnel and session details or summary.
- **tunnel-summary**: Optional. Displays L2TPv3 tunnel summary.
  - {on <DEVICE-NAME>}: Optional. Displays a L2TPv3 tunnel summary on a specified device.
  - <DEVICE-NAME>: Specify the name of AP, wireless controller, or service platform.

Note: For an L2TPv3 tunnel over Auto IPSec, the tunnel status is displayed as: Established (secured by ipsec).

Examples

```
ap7131-11E6C4#show l2tpv3 tunnel-summary
---------------------------------------------------------------------------------------
Sl No  Tunnel Name      Tunnel State            Estd/Total  Sessions   Encapsulation Protocol
---------------------------------------------------------------------------------------
1      testTunnel     Established (secured by ipsec) 1/1  IP
---------------------------------------------------------------------------------------
Total Number of Tunnels 1

ap7131-11E6C4#show l2tpv3
---------------------------------------------------------------------------------------
Tunnel Name : testTunnel
  Control connection id : 2238970979
  Peer Address : 30.1.1.1
  Local Address : 30.1.1.30
  Encapsulation Protocol : IP
  MTU : 1460
  Peer Host Name : rfss
  Peer Vendor Name : Example Company
  Peer Control Connection ID : 322606389
  Tunnel State : Established (secured by ipsec)
  Establishment Criteria : always
  Sequence number of the next msg to the peer : 29
  Expected sequence number of the next msg from the peer : 42
  Sequence number of the next msg expected by the peer : 29
  Retransmission count : 0
  Reconnection count : 0
  Uptime : 0 days 1 hours 2 minutes 47 seconds
---------------------------------------------------------------------------------------
Session Name : session1
  VLANs : 30
  Pseudo Wire Type : Ethernet_VLAN
  Serial number for the session : 6
  Local Session ID : 129538998
  Remote Session ID : 8151374
  Size of local cookie (0, 4 or 8 bytes) : 0
```
First word of local cookie : 0
Second word of local cookie : 0
Size of remote cookie (0, 4 or 8 bytes) : 0
First word of remote cookie : 0
Second word of remote cookie : 0
Session state : Established
Remote End ID : 444
Trunk Session : 1
Native VLAN tagged : Enabled
Native VLAN ID : 0
Number of packets received : 0
Number of bytes received : 0
Number of packets sent : 0
Number of bytes sent : 0
Number of packets dropped : 0
ap7131-11B6C4#
6.1.37 **ldap-agent**

 Displays an LDAP agent's join status (join status to a LDAP server domain)

Use this command When LDAP is specified the external resource (as opposed to local RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials, and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests.

**NOTE:** This command is not available in the USER EXEC Mode.

**Syntax**

```plaintext
show ldap-agent join-status {on <DEVICE-NAME>}
```

**Parameters**

- `show ldap-agent join-status {on <DEVICE-NAME>}`

**Examples**

```plaintext
rfs6000-81701D#show ldap-agent join-status
Primary LDAP Server's agent join-status : Joined domain TEST.
Secondary LDAP Server's agent join-status : Not Configured
rfs6000-81701D#
```
6.1.38 licenses

show commands
Displays installed licenses and usage information

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show licenses {borrowed|lent}

Parameters
- licenses {borrowed|lent} Displays installed licenses and usage information
  - borrowed – Optional. Displays information on licenses borrowed
  - lent – Optional. Displays information on licenses lent

Usage Guidelines
The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single Network Operations Center (NOC) controller. The NOC and the site controllers constitute the first and second tiers of the hierarchy respectively. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy. The site controllers may or may not be grouped to form clusters.

At the time of adoption, access points and adaptive access points are provided license by the adopting controller. These license packs can be installed on both the NOC and site controllers. When a AP/AAP is adopted by a controller, the controller pushes a license on to the device. At this point the various possible scenarios are:
- AP/AAP license packs installed on the NOC controller only.
  - The NOC controller provides the site controllers with the AP licenses, ensuring that per platform limits are not exceeded.
- AP/AAP license packs installed on the NOC and site controllers.
  - The site controller uses its installed licenses and, in case of a shortage, the site controller borrows additional licenses from the NOC. If the NOC controller is unable to allocate sufficient licenses, the site controller unadopts some of the AP/AAPs.
- AP/AAP license packs installed on one controller within a cluster.
  - The site controller shares its installed and borrowed licenses with other cluster controllers.

Examples
rfs4000-229D58#show licenses
Serial Number : 9184521800027

Device Licenses:
  AP-LICENSE
    String       : DEFAULT-6AP-LICENSE
    Value        : 6
    Borrowed     : 0
    Total        : 6
    Used         : 0
  AAP-LICENSE
    String       :
    Value        : 0
    Borrowed     : 0
    Total        : 0
    Used         : 0
The following example shows the show > licenses command output on a NOC controller:

```
nx4500-5CFA2B#show licenses
Serial Number : 6283529900127

Device Licenses:
  AP-LICENSE
    String     : 41a5a30ee9bb0bd7f8d421c001f7c9cfd3cdc66c956ef1f41960aa2a030abb41ac9747a8f0c9f98f
    Value      : 1
  AAP-LICENSE
    String     : 41a5a30ee9bb0bd7f8d421c001f7c9cfd3cdc66c956ef1f41960aa2a030abb41ac9747a8f0c9f98f
    Value      : 1

Total Licenses:
  AP-LICENSE
    Value      : 263
    Used       : 0
  AAP-LICENSE
    Value      : 329
    Used       : 3

Cluster Licenses:
  AP-LICENSE
    Value      : 257
    Used       : 0
  AAP-LICENSE
    Value      : 257
    Used       : 2

Active Members:

<table>
<thead>
<tr>
<th>MEMBER</th>
<th>SERIAL</th>
<th>LIC TYPE</th>
<th>VALUE</th>
<th>LENT</th>
<th>TOTAL</th>
<th>NO.APS</th>
<th>NO.AAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-5C-FA-3B</td>
<td>6283529900127</td>
<td>AP</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>00-15-70-5C-FA-3B</td>
<td>6283529900127</td>
<td>AAP</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Non-Active Members:

<table>
<thead>
<tr>
<th>MEMBER</th>
<th>SERIAL</th>
<th>LIC TYPE</th>
<th>VALUE</th>
<th>LENT</th>
<th>TOTAL</th>
<th>VALIDITY (HRS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-81-70-1D</td>
<td>7295520400017</td>
<td>AP</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>93 days, 5 hours</td>
</tr>
<tr>
<td>00-15-70-81-70-1D</td>
<td>7295520400017</td>
<td>AAP</td>
<td>51</td>
<td>0</td>
<td>51</td>
<td>93 days, 5 hours</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B#
In the following example, the ‘VALIDITY(HRS)’ column specifies the validity period, in days and hours, of a lent license. On a NOC controller, a ‘VALIDITY(HRS)’ value of ‘current’ implies that the site controller is currently adopted. Whereas, a numerical ‘VALIDITY(HRS)’ value indicates the days and hours the lent license is valid for a site controller that is not reachable.

```
rfs7000-37FABE#show licenses lent
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>LENT</th>
<th>BORROWER-MAC</th>
<th>BORROWER-HOST-NAME</th>
<th>VALIDITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-37-FA-BE</td>
<td>rfs7000-37FABE</td>
<td>AP</td>
<td>1</td>
<td>00-00-00-04-04-0A</td>
<td>rfs4000-04040A</td>
<td>93 days, 5 hours</td>
</tr>
<tr>
<td>00-15-70-37-FA-BE</td>
<td>rfs7000-37FABE</td>
<td>AAP</td>
<td>1</td>
<td>00-00-00-04-04-0A</td>
<td>rfs4000-04040A</td>
<td>93 days, 5 hours</td>
</tr>
<tr>
<td>00-15-70-37-FA-BE</td>
<td>rfs7000-37FABE</td>
<td>AAP</td>
<td>1</td>
<td>00-00-00-04-04-0B</td>
<td>rfs4000-04040B</td>
<td>93 days, 5 hours</td>
</tr>
<tr>
<td>00-15-70-37-FA-BE</td>
<td>rfs7000-37FABE</td>
<td>AAP</td>
<td>2</td>
<td>00-23-68-88-1E-4B</td>
<td>rfs4000-881E4B</td>
<td>current</td>
</tr>
<tr>
<td>00-15-70-37-FA-BE</td>
<td>rfs7000-37FABE</td>
<td>AAP</td>
<td>2</td>
<td>00-23-68-88-1E-4B</td>
<td>rfs4000-881E4B</td>
<td>current</td>
</tr>
</tbody>
</table>

```
rfs4000-881E4B#show licenses borrowed
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>BORROWED</th>
<th>VALIDITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-37-FD-89</td>
<td>rfs7000-37FD89</td>
<td>AAP</td>
<td>2</td>
<td>99 days, 23 hours</td>
</tr>
<tr>
<td>00-15-70-81-70-1D</td>
<td>rfs6000-81701D</td>
<td>AP</td>
<td>1</td>
<td>99 days, 23 hours</td>
</tr>
</tbody>
</table>

```
rfs7000-6DCD4B>show licenses borrowed
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>BORROWED</th>
<th>VALIDITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6C-88-09</td>
<td>nx9500-6C8809</td>
<td>AAP</td>
<td>1</td>
<td>00-15-70-81-74-2D</td>
</tr>
<tr>
<td>B4-C7-99-6C-88-09</td>
<td>nx9500-6C8809</td>
<td>AAP</td>
<td>2</td>
<td>B4-C7-99-6D-CD-4B</td>
</tr>
</tbody>
</table>

The following examples show the ‘show > licenses’ output on the devices participating in the process:

```
nx9500-6C8809>show licenses lent
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>LENT</th>
<th>BORROWER-MAC</th>
<th>BORROWER-HOST-NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6C-88-09</td>
<td>nx9500-6C8809</td>
<td>AAP</td>
<td>1</td>
<td>00-15-70-81-74-2D</td>
<td>rfs6000-81742D</td>
</tr>
<tr>
<td>B4-C7-99-6C-88-09</td>
<td>nx9500-6C8809</td>
<td>AAP</td>
<td>2</td>
<td>B4-C7-99-6D-CD-4B</td>
<td>rfs7000-6DCD4B</td>
</tr>
</tbody>
</table>

```
nx9500-6C8809>
```

```
rfs7000-6DCD4B>show licenses borrowed
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>BORROWED</th>
<th>VALIDITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-6C-88-09</td>
<td>nx9500-6C8809</td>
<td>AAP</td>
<td>2</td>
<td>56 days, 6 hours</td>
</tr>
</tbody>
</table>

```
rfs7000-6DCD4B>
```
6-94 WiNG 5.8.1 CLI Reference Guide

6.1.39 lldp

show commands
Displays Link Layer Discovery Protocol (LLDP) information

Supported in the following platforms:
• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show lldp [neighbors|report]
show lldp neighbors {on <DEVICE-NAME>}
show lldp report {detail|on}
show lldp report {detail} {on <DEVICE-OR-DOMAIN-NAME>}

Parameters
• show lldp neighbors {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>lldp</th>
<th>Displays an LLDP neighbors table or aggregated LLDP neighbors table</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbors</td>
<td>Displays an LLDP neighbors table</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays an LLDP neighbors table on a specified device</td>
</tr>
<tr>
<td>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>The following keyword is recursive and common to the ‘report detail’ parameter:</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lldp</th>
<th>Displays an LLDP neighbors table or aggregated LLDP neighbors table</th>
</tr>
</thead>
<tbody>
<tr>
<td>report detail</td>
<td>Displays an aggregated LLDP neighbors table</td>
</tr>
<tr>
<td>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>The following keyword is recursive and common to the ‘report detail’ parameter:</td>
</tr>
<tr>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Displays an aggregated LLDP neighbors table on a specified device or RF Domain</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain</td>
<td></td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config)#show lldp neighbors
-------------------------
Chassis ID: 00-23-68-22-9D-58
System Name: L3-Router
Platform: RFS-4010-00010-WR, Version 5.8.1.0-022D
Capabilities: Bridge  Router
Enabled Capabilities: Bridge  Router
Local Interface: ge1, Port ID (outgoing port): ge2
TTL: 148 sec
Management Addresses: 10.2.0.1,172.18.0.1
rfs7000-37FABE(config)#
6.1.40 logging

Displays the network’s activity log

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show logging \{on <DEVICE-NAME>\}

Parameters

- show logging \{on <DEVICE-NAME>\}

<table>
<thead>
<tr>
<th>logging {on &lt;DEVICE-NAME&gt;}</th>
<th>Displays logging information on a specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Executes the command on a specified device.</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809#show logging

Logging module: enabled
Aggregation time: disabled
Console logging: level debugging
Monitor logging: disabled
Buffered logging: level warnings
Syslog logging: level warnings
Facility: local7

Log Buffer (1666269 bytes):

May 14 05:30:23 2015: nx9500-6C8809 : %DIAG-4-PWRSPLY_FAIL: Power supply failure, no longer redundant
May 14 05:30:13 2015: nx9500-6C8809 : %DEVICE-4-OFFLINE: Device B4-C7-99-74-B4-5C(ap8132-74B45C) is offline, last seen:10 minutes ago on switchport rfs6000-6DB5D4:ge1
May 14 05:20:16 2015: nx9500-6C8809 : %DIAG-4-PWRSPLY_FAIL: Power supply failure, no longer redundant
May 14 05:19:43 2015: nx9500-6C8809 : %DEVICE-4-OFFLINE: Device B4-C7-99-74-B4-5C(ap8132-74B45C) is offline, last seen:10 minutes ago on switchport rfs6000-380649:ge1
--More--
nx9500-6C8809#
6.1.41 mac-access-list

show commands

Displays MAC access list statistics

NOTE: This command is not present in USER EXEC mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show mac-access-list stats {<MAC-ACCESS-LIST-NAME>|on}
show mac-access-list stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}

Parameters

- show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}

Examples

nx6524-5483B0#show mac-access-list stats scalemacacl | i 311
permit D0-67-E5-3F-C0-00 FF-FF-FF-FF-F0-00 host 00-1E-EC-F2-0A-76 rule-precedence 311
Hitcount: 0        Hardware Hitcount: 0
nx6524-5483B0#
6.1.42 **mac-address-table**

- **show commands**

Displays MAC address table entries

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show mac-address-table {on <DEVICE-NAME>}
```

**Parameters**

- `show mac-address-table {on <DEVICE-NAME>}`

**Examples**

```
rfs7000-6DCD4B(config)#show mac-address-table
BRIDGE VLAN PORT          MAC              STATE
----------------------------------------------------
1  192  ge2              00-23-68-13-9B-34 forward
1  1    ge1              00-23-68-22-9D-58 forward
1  192  ge2              00-A0-F8-68-D5-65 forward
1  192  ge2              B4-C7-99-5C-FA-2B forward
1  192  ge2              3C-CE-73-F4-47-83 forward
1  1    ge1              00-23-68-22-9D-5A forward
1  192  ge2              00-15-70-38-06-49 forward
1  192  ge2              00-0F-8F-19-BA-4C forward
1  192  ge2              B4-C7-99-58-72-58 forward
1  192  ge2              00-23-68-11-E6-C4 forward
1  192  ge2              B4-C7-99-6C-88-09 forward
1  192  ge2              5C-0E-8B-18-10-91 forward
1  192  ge2              B4-C7-99-5C-FA-8E forward
1  1    ext-vlan         00-A0-F8-67-1D-17 forward
1  192  ge2              00-23-68-88-0D-A7 forward
1  192  ge2              00-04-96-43-4C-AA forward
1  192  ge2              00-15-70-37-FD-F2 forward
1  192  ge2              B4-C7-99-74-B4-5C forward
1  192  ge2              B4-C7-99-6D-B5-D4 forward
1  192  ge2              00-02-B3-28-D1-55 forward
```

Total number of MACs displayed: 20
```
rfs7000-6DCD4B(config)#
```
6.1.43 mac-auth

Displays details of wired ports that have MAC address authentication enabled.

Use this command to view MAC authentication configuration and authentication state. The command displays the current authentication state of the wired host, the authorization state of the Ge1 port, and the wired hosts’ MAC address. The port status displays as Authorized if the wired host has successfully authenticated and Not Authorized if the wired host has not authenticated or has failed MAC authentication.

For more information on enabling MAC address authentication on a wired port, see mac-auth.

Supported in the following platforms:
- Access Points — AP6511
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

```
show mac-auth {all|interface|on}
show mac-auth {all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel <1-3>|t1e1 <1-4>|up <1-2]|vmif <1-X>|xge <1-4>]} {on <DEVICE-NAME>}
```

Parameters

- **show mac-auth {all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel <1-3>|t1e1 <1-4>|up <1-2]|vmif <1-X>|xge <1-4>]} {on <DEVICE-NAME>}

  - **mac-auth** Displays MAC authentication related information for all interfaces or all interfaces
  - **all** Optional. Displays MAC authentication related information for all interfaces
  - **interface** Optional. Displays MAC authentication related information for a specified interface. Specify the interface using one of the following options:
    - **<INTERFACE-NAME>** – Selects the interface identified by the <INTERFACE-NAME> keyword
    - **ge <1-5>** – Selects the GigabitEthernet interface identified by the index number
    - **port-channel <1-3>** – Selects the port channel interface identified by the index number
    - **t1e1 <1-4>** – Selects the layer 2 interface (Ethernet port)
    - **up <1-2>** – Selects the WAN Ethernet interface identified by the index number
    - **vmif <1-X>** – Selects the virtual machine interface (VMIF) identified by the index number
    - **xge <1-4>** – Selects the TenGigabitEthernet interface identified by the index number
  - **on <DEVICE-NAME>** The following keywords are common to the 'all' and 'interface' parameters:
    - **on <DEVICE-NAME>** – Optional. Displays MAC authentication related information on a specified device
    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

**Note:** When the ‘on’ keyword is used exclusively, without the ‘all’ and ‘interface’ options, the system displays MAC authentication related information for interfaces configured on the specified device.
Examples
rfs4000-229D58(config)#show mac-auth all
AAA-Policy is none

Mac Auth info for interface GE1
-----------------------------------
  Mac Auth Enabled
  Mac Auth Not Authorized

Mac Auth info for interface GE2
-----------------------------------
  Mac Auth Disabled
  Mac Auth Not Authorized

Mac Auth info for interface GE3
-----------------------------------
  Mac Auth Disabled
  Mac Auth Not Authorized

Mac Auth info for interface GE4
-----------------------------------
  Mac Auth Disabled
  Mac Auth Authorized

Mac Auth info for interface GE5
-----------------------------------
  Mac Auth Disabled
  Mac Auth Not Authorized

Mac Auth info for interface UP1
-----------------------------------
  Mac Auth Disabled
  Mac Auth Not Authorized

rfs4000-229D58(config)#
### 6.1.44 mac-auth-clients

- **show commands**

Displays MAC authenticated clients

Supported in the following platforms:
- Access Points — AP6511
- Wireless Controllers — RFS4000, RFS6000, RFS7000

#### Syntax

```plaintext
show mac-auth-clients [all|interface]
show mac-auth-clients all {on <DEVICE-NAME>}
show mac-auth-clients interface {<INF-NAME>|ge <1-X>|port-channel <1-2>|vmif <1-8>|xge <1-4>}
```

#### Parameters

- **show mac-auth-clients all {on <DEVICE-NAME>}

- **show mac-auth-clients interface {<INF-NAME>|ge <1-X>|port-channel <1-2>|vmif <1-8>|xge <1-4>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-auth-clients</td>
<td>Displays MAC authenticated clients based on the parameters passed. The options are: all and interface.</td>
</tr>
<tr>
<td>all</td>
<td>Displays MAC authenticated clients for all interfaces</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays MAC authenticated clients for all interfaces on a specified device</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Displays MAC authenticated clients for the specified interface. Select the interface type from the following options:</td>
</tr>
<tr>
<td>&lt;INF-NAME&gt;</td>
<td>Specify the interface name.</td>
</tr>
<tr>
<td>ge &lt;1-X&gt;</td>
<td>Displays MAC authenticated clients for the selected GigabitEthernet interface. Specify the GE interface index from 1 - X. This will vary for different device types.</td>
</tr>
<tr>
<td>port-channel &lt;1-2&gt;</td>
<td>Displays MAC authenticated clients for the selected port channel interface. Specify the port channel interface index from 1 - 2.</td>
</tr>
<tr>
<td>vmif &lt;1-8&gt;</td>
<td>Displays MAC authenticated clients for the selected virtual machine (VM) interface. Specify the VM interface index from 1 - 8.</td>
</tr>
<tr>
<td>xge &lt;1-4&gt;</td>
<td>Displays MAC authenticated clients for the selected TenGigabitEthernet interface. Specify the interface index from 1 - 4.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays MAC authenticated clients for the specified interface on a specified device</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>
Examples

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show mac-auth-clients interface ge 1
-----------------------------------------------
MAC               STATE            INTERFACE
-----------------------------------------------
-----------------------------------------------
Total number of MACs displayed: 0
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
6.1.45 mint

▶ show commands

Displays MiNT protocol configuration commands

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show mint [config|dis|id|info|known-adopters|links|lsp|lsp-db|mlcp|neighbors|route|stats|tunnel-controller|tunneled-vlans] {on <DEVICE-NAME>}
show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on <DEVICE-NAME>}
show mint [dis|links|neighbors|tunnel-controller] {details} {on <DEVICE-NAME>}
show mint lsp
show mint lsp-db {details <MINT-ADDRESS>} {on <DEVICE-NAME>}

Parameters
- show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mint</td>
<td>Displays MiNT protocol information based on the parameters passed</td>
</tr>
<tr>
<td>config</td>
<td>Displays MiNT configuration</td>
</tr>
<tr>
<td>id</td>
<td>Displays local MiNT ID</td>
</tr>
<tr>
<td>info</td>
<td>Displays MiNT status</td>
</tr>
<tr>
<td>known-adopters</td>
<td>Displays known, possible, or reachable adopters</td>
</tr>
<tr>
<td>route</td>
<td>Displays MiNT route table details</td>
</tr>
<tr>
<td>stats</td>
<td>Displays MiNT related statistics</td>
</tr>
<tr>
<td>tunneled-vlans</td>
<td>Displays MiNT tunneled VLAN details</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays MiNT protocol details on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- show mint [dis|links|neighbors|tunnel-controller] {details} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mint</td>
<td>Displays MiNT protocol information based on the parameters passed</td>
</tr>
<tr>
<td>dis</td>
<td>Displays MiNT network Designated Intermediate Systems (DISes) and Ethernet Virtualization Interconnects (EVISes)</td>
</tr>
<tr>
<td>links</td>
<td>Displays MiNT networking link details</td>
</tr>
<tr>
<td>neighbors</td>
<td>Displays adjacent MiNT peer details</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show mint lsp {details &lt;MINT-ADDRESS&gt;} {(on &lt;DEVICE-NAME&gt;)}</code></td>
<td>Displays this router’s MiNT Label Switched Paths (LSPs)</td>
</tr>
<tr>
<td><code>show mint lsp-db {details &lt;MINT-ADDRESS&gt;} {(on &lt;DEVICE-NAME&gt;)}</code></td>
<td>Displays MiNT LSP database entries</td>
</tr>
<tr>
<td><code>show mint mlcp {history} {(on &lt;DEVICE-NAME&gt;)}</code></td>
<td>Displays IPv4 and IPv6 MiNT Link Creation Protocol (MLCP) status</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config)#show mint stats
0 L1 neighbors
L1 LSP DB size 1 LSPs (0 KB)
1 L1 routes
Last SPF's took 0s
SPF (re)calculated 1 times.
levels 1
base priority 180
dis priority 180
rfs7000-37FABE(config)#
```
rfs7000-37FABE(config)#show mint lsp
id 70.37.fa.be, level 1, seqnum 18640, 0 adjacencies, 0 extended-vlans,
expires in 1145 seconds, republish in 722 seconds, changed True,
ext-vlan FDB pri 0, 180 bytes

rfs7000-37FABE(config)#show mint lsp-db
1 LSPs in LSP-db of 70.37.FA.BE:
LSP 70.37.FA.BE at level 1, hostname "rfs7000-37FABE", 0 adjacencies, seqnum 84941

rfs7000-37FABE(config)#show mint route
Destination : Next-Hop(s)
70.37.FA.BE : 70.37.FA.BE via self

rfs7000-37FABE(config)#show mint known-adopters
70.37.FA.BE

rfs7000-37FABE(config)#show mint config
Base priority 180
DIS priority 180
Control priority 180
UDP/IP Mint encapsulation port 24576
Global Mint MTU 1500

ap7532-15E6E4#show mint mlcp
MLCP VLAN state: MLCP_DONE
Potential VLAN links: 1
All VLANs were scanned 2 times
Link created on VLAN 1
MLCP IP state: MLCP_DISCOVERING
Potential L3 Links:
192.168.1.43
MCLP IP Hello Interval: 15s(default), Adjacency hold time: 46s(default)
MCLP VLAN Hello Interval: 4s(default), Adjacency hold time: 13s(default)
ap7532-15E6E4#
6.1.46 ntp

Displays Network Time Protocol (NTP) information. NTP enables clock synchronization within a network.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show ntp [associations|status]
show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]  

Parameters

- show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]  

| ntp associations {detail|on} | Displays existing NTP associations. The interaction between the controller or service platform and a SNTP server constitutes an association. SNTP associations are of two kinds:
| OFFSET | DISPERSION |
| 0.0 | 15937.5 |
| 0.0 | 15937.5 |
| 0.0 | 15937.5 |

| ntp status {on <DEVICE-NAME>} | Displays the performance (status) information relative to the NTP association status. Use this command to view the access point, controller, or service platform’s current NTP resource. Use this command to view the access point, controller, or service platform’s current NTP resource. |
| STATUS | NTP SERVER IP ADDR | REF CLOCK | IP ADDR | STRATUM | WHEN | POLL | REACH | DELAY |
| 0.0 | 12.12.12.12 | INIT | 16 | - | 1024 | 0 | 0.0 |
| 0.0 | 11.11.11.11 | INIT | 16 | - | 1024 | 0 | 0.0 |
| 0.0 | 10.10.10.10 | INIT | 16 | - | 1024 | 0 | 0.0 |

Note: If the ‘on’ keyword is used without the ‘detail’ keyword, the system displays a summary of existing NTP associations on the specified device or RF Domain.

Examples

nx9500-6C8809#show ntp associations

| STATUS | NTP SERVER IP ADDR | REF CLOCK | IP ADDR | STRATUM | WHEN | POLL | REACH | DELAY |
| 0.0 | 12.12.12.12 | INIT | 16 | - | 1024 | 0 | 0.0 |
| 0.0 | 11.11.11.11 | INIT | 16 | - | 1024 | 0 | 0.0 |
| 0.0 | 10.10.10.10 | INIT | 16 | - | 1024 | 0 | 0.0 |

STATUS Notation: * master (synced), # master (unsynced), + selected, - candidate, - configured
nx9500-6C8809#

nx9500-6C8809#show ntp status

<table>
<thead>
<tr>
<th>ITEM</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leap</td>
<td>Clock is unsynchronized</td>
</tr>
<tr>
<td>Stratum</td>
<td>16</td>
</tr>
<tr>
<td>Reference</td>
<td>INIT</td>
</tr>
<tr>
<td>Frequency</td>
<td>0.0000 Hz</td>
</tr>
<tr>
<td>Precision</td>
<td>2^-20</td>
</tr>
<tr>
<td>Reference time</td>
<td>00000000.00000000 (Feb 07 11:58:16 UTC 2036)</td>
</tr>
<tr>
<td>Clock Offset</td>
<td>0.000 msec</td>
</tr>
<tr>
<td>Root delay</td>
<td>0.000 msec</td>
</tr>
<tr>
<td>Root Dispersion</td>
<td>0.000 msec</td>
</tr>
</tbody>
</table>

nx9500-6C8809#
6.1.47 password-encryption

Displays password encryption status (enabled/disabled)

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show password-encryption status

Parameters
- show password-encryption status

| password-encryption status | Displays password encryption status (enabled/disabled) |

Examples
rfs7000-37FABE(config)#show password-encryption status
Password encryption is enabled
rfs7000-37FABE(config)#
### 6.1.48 `pppoe-client`

#### show commands

Displays **Point-to-Point Protocol over Ethernet** (PPPoE) client information

Use this command to view PPPoE statistics derived from access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables point-to-points connection to an ISP over existing Ethernet interface.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

#### Parameters

- `configuration` Displays detailed PPPoE client configuration
- `status` Displays detailed PPPoE client status
- `on <DEVICE-NAME>` The following keywords are common to ‘configuration’ and ‘status’ parameters:
  - `on <DEVICE-NAME>` – Optional. Displays detailed PPPoE client status or configuration on a specified device
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

#### Examples

```
rfs7000-37FABE(config)#show pppoe-client configuration
PPPoE Client Configuration:
+-------------------------------------------
| Mode          : Disabled                  |
| Service Name  :                        |
| Auth Type     : pap                      |
| Username      :                        |
| Password      :                        |
| Idle Time     : 600                      |
| Keepalive     : Disabled                 |
| Local n/w     : vlan1                    |
| Static IP     : 0.0.0.0                  |
| MTU           : 1492                      |
+-------------------------------------------
```

```
rfs7000-37FABE(config)#
```
6.1.49 privilege

> show commands

Displays a device's existing privilege level

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show privilege

Parameters

None

Examples

rfs7000-37FABE(config)#show privilege
Current user privilege: superuser
rfs7000-37FABE(config)#
6.1.50 radius

`show commands`

Displays the amount of access time consumed and the amount of access time remaining for all guest users configured on a RADIUS server.

Every captive portal guest user can access the captive portal for a specified duration. This results in following three scenarios:

- Scenario 1: Access duration not specified (in this case the default of 1440 minutes is applied)
- Scenario 2: Access duration is specified and is greater than 0
- Scenario 3: Access duration is specified and equals to 0 (in this case the guest user has unlimited access)

In all the three scenarios the access time consumed is the duration for which the guest user has logged. But the access time remaining varies. It is calculated as follows:

- Scenarios 1 & 2 - It is the lesser of the following two values: difference between the configured access duration and the time consumed AND the time until user account expiration.
- Scenario 3 - It is the time until user account expiration

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show radius guest-users {<GUEST-USER-NAME>}`

**Parameters**

- `show radius guest-users {<GUEST-USER-NAME>}`

<table>
<thead>
<tr>
<th>radius guest-users {&lt;GUEST-USER-NAME&gt;}</th>
<th>Displays RADIUS server’s guest user’s access details: total time for which the user has logged in, and the amount of access time remaining.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;GUEST-USER-NAME&gt;</code> – Optional. Provide the name of the guest user (whose access details are to be viewed). If no name is provided, the system displays details of all guest users who have successfully logged in at least once.</td>
</tr>
<tr>
<td></td>
<td>Use this command in the captive-portal context to view time and data statistics for guest user(s) having bandwidth-based or time-based vouchers configured. In such a scenario, the system displays the following information: data configured, data remaining, configured and current bandwidths (for both downlink and uplink), time configured, and time remaining. If bandwidth-based voucher is not applicable to a guest user, the data configured and data remaining values are displayed as 'unlimited'. The bandwidth columns are blank. If time-based voucher is not applicable to a guest user, the only value displayed is the time remaining (which is the time till the expiration of the guest user’s account).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For more information on configuring bandwidth-based and time-based vouchers, see <code>user</code>.</td>
</tr>
</tbody>
</table>
Examples
rfs4000-229D58#show radius guest-users

```
TIME (min:sec)  USED    REMAINING   GUEST USER
0:00         9:00   time9
0:00         5:00   time5
0:00        15:00   time15
0:00    305416:35   notime
2:31         7:29   time10
```
rfs4000-229D58#

The following example shows a RADIUS user pool with guest users having bandwidth-based, time-based, bandwidth and time based, and no bandwidth or time based vouchers:

```
rfs4000-229D58(config-captive-portal-wdws)#show context
radius-user-pool-policy wdws
  user time_and_data password 0 both group wdws guest expiry-time 12:00 expiry-date 12/31/2015 access-duration 8000 data-limit 500 committed-downlink 3000 committed-uplink 2000 reduced-downlink 1000 reduce4
  user neither password 0 nine group wdws guest expiry-time 12:00 expiry-date 12/31/2015
  user data_only password 0 data group wdws guest expiry-time 12:00 expiry-date 12/31/2015 data-limit 125 committed-downlink 1000 committed-uplink 800 reduced-downlink 500 reduced-uplink 400
  user time_only password 0 time group wdws guest expiry-time 12:00 expiry-date 12/31/2015 access-duration 5000
rfs4000-229D58(config-captive-portal-wdws)#
```

The following example shows the captive portal access details for the above mentioned RADIUS user pool users:

```
rfs4000-229D58(config-captive-portal-wdws)#show radius guest-users

```
```
GUEST USER   TIME (DD:HH:MM:SS)   DATA (kilobytes)   BANDWIDTH (kbps)
  DN  CFGD DN  CURREN DN  CFGD UP  CURR DN  CFGD DN  CURREN DN  CFGD DN  CURREN
```
```
time_and_data  5:13:20:00  5:12:00:50
neither         till expiry 221:19:44:54
2000           until expiry
```
```
data_only  512000  433727
800             127587
```
```
time_only     3:11:20:00  3:11:19:47
800             127587
```
```
```
```
```
Current time: 17:15:07
rfs4000-229D58(config-captive-portal-wdws)#
```
6.1.51 `reload`

Displays scheduled reload information for a specific device

```plaintext
NOTE: This command is not present in the USER EXEC mode.
```

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**
- `show reload {on <DEVICE-OR-DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>reload {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</th>
<th>Displays scheduled reload information for a specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays configuration on a specified device</td>
<td></td>
</tr>
<tr>
<td>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**
```
rfs7000-37FABE(config)#show reload
No reload is scheduled.
rfs7000-37FABE(config)#
```
6.1.52 rf-domain-manager

Displays RF Domain manager selection details

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
show rf-domain-manager
```

**Parameters**

- `on <DEVICE-OR-DOMAIN-NAME>`

<table>
<thead>
<tr>
<th>rf-domain-manager</th>
<th>Displays RF Domain manager selection details</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Displays RF Domain manager selection details on a specified device or domain</td>
</tr>
</tbody>
</table>

| <DEVICE-OR-DOMAIN-NAME> | - specify the name of the AP, wireless controller, service platform, or RF Domain. |

**Examples**

```
rfs7000-37FABE(config)#show rf-domain-manager
RF Domain RFDOMAIN_TechPubsLabLan
RF Domain Manager:
    ID: 70.37.FA.BE
    Priority: 180
    Has IP MiNT link
    Has wired MiNT links
Device under query:
    Priority: 180
    Has IP MiNT links
    Has wired MiNT links
rfs7000-37FABE(config)#
```
6.1.53 role

show commands

Displays role based firewall information

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show role [ldap-stats|wireless-clients]
show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}

Parameters

- show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>role ldap-stats</th>
<th>Displays LDAP server status and statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>role wireless-clients</td>
<td>Displays clients associated with roles</td>
</tr>
</tbody>
</table>

on <DEVICE-NAME>

The following parameters are common to the 'ldap-stats' and 'wireless-clients' keywords:

- on <DEVICE-NAME> – Optional. Displays clients associated with roles on a specified device
- <DEVICE-NAME> – Specify the name of the AP, wireless controller, and service platform.

Examples

rfs7000-37FABE(config)#show role wireless-clients
No ROLE statistics found.
rfs7000-37FABE(config)#
### 6.1.54 route-maps

- **show commands**
  - Displays route map statistics for defined device routes

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show route-maps {on <DEVICE-NAME>}
```

**Parameters**

- `show route-maps {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-maps</td>
<td>Displays configured route map statistics for all defined routes</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>For more information on route maps, see <a href="#">route-map on page 24-6</a>.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays route map statistics on a specified device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs7000-37FABE(config)#show route-maps
rfs7000-37FABE(config)#
```
### 6.1.55 rtls

Display the Real Time Location Service (RTLS) statistics for access points contributing locationing information.

#### Supported Platforms
- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
show rtls [aeroscout|ekahau] {<MAC/HOSTNAME>} {on <DEVICE-OR-DOMAIN-NAME>}
```

#### Parameters
- **rtls**
  - Displays access point RTLS statistics
- **aeroscout**
  - Displays access point Aeroscout statistics
- **ekahau**
  - Displays access point Ekahau statistics
- **<MAC/HOSTNAME>**
  - Optional. Displays Aeroscout or Ekahau statistics for a specified access point. Specify the MAC address or hostname of the access point.
- **on <DEVICE-OR-DOMAIN-NAME>**
  - The following keyword is recursive and common to ‘Aeroscout’ and ‘Ekahau’ parameters:
    - **on <DEVICE-OR-DOMAIN-NAME>**
      - Optional. Displays Aeroscout or Ekahau statistics on a specified device or domain.
    - **<DEVICE-OR-DOMAIN-NAME>**
      - Specify the name of the AP, wireless controller, service platform, or RF Domain.

#### Examples

```
rfs4000-229D58(config)#show rtls aeroscout

Aeroscout Engine IP: 0.0.0.0 Port: 0
Send Count : 0
Recv Count : 0
Tag Reports : 0
Nacks : 0
Acks : 0
Lbs : 0
AP Status : 0
AP Notif : 0
Send Err : 0
Errmsg Count : 0

Total number of APs displayed: 1
rfs4000-229D58(config)#
```
6.1.56 **running-config**

Displays configuration files (where all configured MAC and IP access lists are applied to an interface)

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show running-config {aaa-policy|application|application-policy|association-acl-policy|auto-provisioning-policy|captcha-portal-policy|device|device-overrides|dhcp-server-policy|dhcv6-server-policy|ex3500-management-policy|ex3500-qos-class-map-policy|ex3500-qos-policy-map|firewall-policy|guest-management-policy|include-factory|interface|ip-access-list|ipv6-access-list|mac-access-list|management-policy|nsight-policy|radio-qos-policy|rf-domain|roaming-assist-policy|smart-cache-policy|smart-rf-policy|url-filter|url-list|web-filter-policy|wlan|wlan-qos-policy} {include-factory}
```

```
```

```
show running-config {device {<MAC>|self}} {include-factory}
```

```
show running-config {device-overrides {brief}}
```

```
show running-config {include-factory}
```

```
show running-config {interface} {<INTERFACE-NAME>|ge|include-factory|me|port-channel|pppoel|vlan|wwan1}
```

```
show running-config {interface} {<INTERFACE-NAME>|ge <1-4>|include-factory|me1|port-channel <1-2>|pppoel|vlan <1-4094>|wwan1} {include-factory}
```

```
show running-config {ip-access-list <IP-ACCESS-LIST-NAME>|ipv6-access-list <IPV6-ACCESS-LIST-NAME>|mac-access-list <MAC-ACCESS-LIST-NAME} {include-factory}
```

```
show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}
```

```
show running-config {profile [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5550|nx65xx|nx75xx|nx9000|nx9600} {include-factory}
```

```
show running-config {rf-domain <DOMAIN-NAME>} {include-factory}
```

```
show running-config {wlan <WLAN-NAME>} {include-factory}
```

```
show running-config url-filter <URL-FILTER-NAME>
```

```
show running-config url-list <URL-LIST-NAME} {include-factory}
```
### Parameters


- **show running-config** *(device [<MAC>|self]) {include-factory}

- **show running-config** *(device-overrides {brief})

- **show running-config** *(include-factory)

| running-config | Optional. Displays current running configuration
|----------------|------------------------------------------------------------------------------------------------------------------|
| device [<MAC>|self] | Optional. Displays device configuration
| include-factory | The following keyword is common to all policies:
| brief | Optional. Displays a brief summary of device overrides

| include-factory | Optional. Includes factory defaults

### running-config

- **<POLICY-TYPE> <POLICY-NAME>**
  - Optional. Select the policy type, for example, aaa-policy, auto-provisioning-policy, captive-portal-policy etc., and then specify the policy name. The system displays the selected policy’s configuration.
  - **<POLICY-TYPE>**
  - **<POLICY-NAME>** – Specify the name of the policy (should be existing and configured).

- **include-factory**
  - Optional. Includes factory defaults

### device

- **device [<MAC>|self]**
  - Displays a specified device configuration. Specify the MAC address of the device.
  - **<MAC>** – Displays a specified device configuration. Specify the MAC address of the device.
  - **self** – Displays the logged device’s configuration

- **include-factory**
  - The following keyword is common to the `<MAC>` and ‘self’ parameters:
  - **Optional. Displays factory defaults**

### device-overrides

- **device-overrides {brief}**

- **brief** – Optional. Displays a brief summary of device overrides

### interface

- **interface**
  - Optional. Displays interface configuration
  - **<INTERFACE-NAME>**

- **include-factory**
  - Optional. Displays a specified interface configuration. Specify the interface name.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Displays current running configuration. Optionally, you can execute the command along with one of the associated keywords to view the running configuration for that top-level object. To view a access-list and its configuration, specify the ACL type and provide the ACL name. <strong>Note:</strong> If the command is executed without a keyword, the system displays the entire running configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show running-config {ip-access-list &lt;IP-ACCESS-LIST-NAME&gt;</td>
<td>ipv6-access-list &lt;IPv6-ACCESS-LIST-NAME&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config {meshpoint &lt;MESHPOINT-NAME&gt;} {include-factory}</code></td>
<td>Displays meshpoint configuration. Optional. Includes factory defaults along with running configuration details.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show running-config {profile [anyap</td>
<td>ap621</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays current running configuration</td>
</tr>
<tr>
<td><code>rf-domain &lt;DOMAIN-NAME&gt;</code></td>
<td>Optional. Displays current configuration for a RF Domain</td>
</tr>
<tr>
<td>include-factory</td>
<td>Optional. Includes factory defaults</td>
</tr>
<tr>
<td><code>wlan &lt;WLAN-NAME&gt;</code></td>
<td>Optional. Displays current configuration for a WLAN</td>
</tr>
<tr>
<td>include-factory</td>
<td>Optional. Includes factory defaults</td>
</tr>
<tr>
<td><code>url-filter &lt;URL-FILTER-NAME&gt;</code></td>
<td>Optional. Displays current configuration for the URL filter identified by the &lt;URL-FILTER-NAME&gt; keyword</td>
</tr>
<tr>
<td>include-factory</td>
<td>Optional. Includes factory defaults</td>
</tr>
<tr>
<td><code>url-list &lt;URL-LIST-NAME&gt;</code></td>
<td>Optional. Displays current configuration for the URL list identified by the &lt;URL-LIST-NAME&gt; keyword</td>
</tr>
<tr>
<td>include-factory</td>
<td>Optional. Includes factory defaults</td>
</tr>
</tbody>
</table>

**profile**

<table>
<thead>
<tr>
<th><code>&lt;DEVICE-TYPE&gt;</code></th>
<th><code>&lt;PROFILE-NAME&gt;</code></th>
<th>Optional. Displays current configuration for a specified profile. Select the device type, and then specify the profile name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DEVICE-TYPE&gt;</code></td>
<td></td>
<td>• <code>&lt;DEVICE-TYPE&gt;</code> – Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600.</td>
</tr>
</tbody>
</table>
| `<PROFILE-NAME>`|                  | • `<PROFILE-NAME>` – Specify the profile name for the selected `<DEVICE-TYPE>`.

**Note:** Select the ‘anyap’ option to view the running configuration of any type of device.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>include-factory</code></td>
<td>Optional. This parameter is common to all profiles. When selected, it includes factory defaults in the output.</td>
</tr>
</tbody>
</table>

- `profile <DEVICE-TYPE> <PROFILE-NAME>`
- `include-factory`
Examples

rfs7000-37FABE(config)#show running-config device self
!
firewall ratelimit-trust policy default
!
management-policy default
telnet
http server
ssh
!
firewall-policy default
!
mint-security-policy the_policy
  rejoin-timeout 35
!
device-discover-policy default
!
rfs7000 00-15-70-37-FA-BE
  hostname rfs7000-37FABE
  no country-code
  bridge vlan 3
  bridge vlan 5
  ip dhcp trust
  ip igmp snooping querier version 2
  ip igmp snooping querier max-response-time 3
  ip igmp snooping querier timer expiry 89
  wep-shared-key-auth
  radius nas-identifier test
--More--
rfs7000-37FABE(config)

nx6500-31FABE(config)#show running-config device 11-22-33-44-55-66 include-factory
!
radio-qos-policy default
  wmm best-effort aifsn 3
  wmm video txop-limit 94
  wmm video aifsn 1
  wmm video cw-min 3
  wmm video cw-max 4
  wmm voice txop-limit 47
  wmm voice aifsn 1
  wmm voice cw-min 2
--More--
nx6500-31FABE(config)#

rfs7000-6DCD4B#show running-config profile ap81xx default-ap81xx
profile ap81xx default-ap81xx
  autoinstall configuration
  autoinstall firmware
  crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
  crypto remote-vpn-client
  interface radio1
  interface radio2
  interface radio3
  interface ge1
  interface ge2
  interface vlan1
--More--
rfs7000-6DCD4B#

nx9500-6C8809#show running-config url-filter URL_FILTER_Shopping include-factory
url-filter URL_FILTER_Shoping
  no description
blacklist category-type p2p precedence 20 description description
blacklist category-type news-sports-general category shopping precedence 10 description description
  blockpage path internal
  blockpage internal org-name Your Organization Name
  blockpage internal org-signature Your Organization Name, All Rights Reserved.
  blockpage internal title This URL may have been filtered.
  blockpage internal footer If you have any questions please contact your IT department.
  blockpage internal content The site you have attempted to reach may be considered inappropriate for access.
  no blockpage internal main-logo
  no blockpage internal small-logo
  no blockpage external
nx9500-6C8809#

nx9500-6C8809#show running-config url-list AllowedShopping
url-list AllowedShopping
  url ebay.com depth 10
  url amazon.com depth 10
nx9500-6C8809#

nx9500-6C8809#show running-config application Bing
application Bing
  app-category streaming
  use url-list Bing
nx9500-6C8809#
6.1.57 session-changes

show commands

Displays configuration changes made in the current session

Supported in the following platforms:
  • Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  • Wireless Controllers — RFS4000, RFS6000, RFS7000
  • Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show session-changes

Parameters
None

Examples
rfs7000-37FABE(config)#show session-changes

No changes in this session

rfs7000-37FABE(config)#
6.1.58 session-config

Show commands

Lists active open sessions on a device

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show session-config {include-factory}

Parameters

- session-config
- include-factory

<table>
<thead>
<tr>
<th>session-config</th>
<th>Displays current session configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>include-factory</td>
<td>Optional. Includes factory defaults</td>
</tr>
</tbody>
</table>

Examples

nx4500-5CFA2B(config)#show session-config

! Configuration of NX4500 version 5.8.1.0-037B
!
! version 2.3
!
! url-list AllowedShopping
! url ebay.com depth 10
! url amazon.com depth 10
!
! url-list test
! description This URL list contains social communication URLs
! url https://www.facebook.com depth 5
!
! url-filter WebFilter_ShoppingSites
! whitelist url-list AllowedShopping precedence 2 description description
! blacklist category-type news-sports-general category shopping precedence 1 description description
!
! firewall-policy default
! no ip dos tcp-sequence-past-window
! alg sip
--More--
nx4500-5CFA2B(config)#
**6.1.59 sessions**

- **show commands**

Displays CLI sessions initiated on a device

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show sessions {on <DEVICE-NAME>}`

**Parameters**

- `show sessions {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Displays CLI sessions initiated on a device</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays CLI sessions on a specified device</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt;</td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Examples**

```
x4500-5CFA2B>show sessions
INDEX  COOKIE  NAME      START TIME            FROM               ROLE
1      4       snmp      2015-06-08 08:47:29   127.0.0.1          superuser
2      5       snmp2     2015-06-08 08:47:29   127.0.0.1          superuser
3      27      admin     2015-06-11 08:42:43   192.168.100.109    superuser
```

nx4500-5CFA2B>
6.1.60 site-config-diff

Displays the difference in site configuration available on the NOC and a site.

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single Network Operations Center (NOC) controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

NOC controllers possess default site configuration details. Overrides applied at the site level result in a mismatch of configuration at the site and the default site configuration available on the NOC controller. Use this command to view this difference.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show site-config-diff <SITE-NAME>

Parameters

- show site-config-diff <SITE-NAME>

Examples

nx9500-6C874D#show site-config-diff 5C-0E-8B-18-06-F4
---- Config diff for switch 5C-0E-8B-18-06-F4 ----
rfs6000 5C-0E-8B-18-06-F4
interface pppoe1
  no shutdown
nx9500-6C874D#
6.1.61 smart-rf

show commands

Displays Self-Monitoring At Run Time (Smart RF) statistical history to assess adjustments made to device configurations to compensate for detected coverage holes or device failures

When invoked by an administrator, Smart RF instructs access point radios to change to a specific channel and begin beaoming using the maximum available transmit power. Within a well-planned deployment, any RF Domain member access point radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, un-managed radios. AP-to-AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show smart-rf [ap|channel-distribution|history|history-timeline|interfering-ap|interfering-neighbors|radio]

show smart-rf ap {<MAC>|<DEVICE-NAME>|activity|energy|neighbors|on <DOMAIN-NAME>}
show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
show smart-rf ap {activity|energy|neighbors} [<MAC>|<DEVICE-NAME>] {on <DOMAIN-NAME>}

show smart-rf [channel-distribution|history|history-timeline] {on <DOMAIN-NAME>}

show smart-rf radio {<MAC>|activity|all-11an|all-11bgn|channel|energy|neighbors|on <DOMAIN-NAME>}
show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}
show smart-rf radio {activity|neighbors} [<MAC]|all-11an|all-11bgn} {on <DOMAIN-NAME>}

show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}
show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>|threshold <50-100>}

Parameters

- show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}

<table>
<thead>
<tr>
<th>smart-rf</th>
<th>Displays Smart RF related information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>Displays access point related Smart RF information</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Optional. Uses MAC addresses to identify access points. Displays all access points, if no MAC address is specified.</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Optional. Uses an administrator defined name to identify an access point</td>
</tr>
<tr>
<td>on &lt;DOMAIN-NAME&gt;</td>
<td>Optional. Displays access point details on a specified RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DOMAIN-NAME&gt; — Specify the domain name.</td>
</tr>
</tbody>
</table>

| show smart-rf ap (activity|energy|neighbors) [<MAC]|<DEVICE-NAME>] {on <DOMAIN-NAME>}) |

<table>
<thead>
<tr>
<th>smart-rf</th>
<th>Displays Smart RF related information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>Displays AP related Smart RF information</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show smart-rf</code></td>
<td>Displays Smart RF related information</td>
</tr>
<tr>
<td></td>
<td>• <code>channel-distribution</code> - Displays Smart RF channel distribution information. This provides an overview of how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF Domain member device performance.</td>
</tr>
<tr>
<td></td>
<td>• <code>history</code> - Displays Smart RF calibration history. Use this option to view description and types of Smart RF events impacting RF Domain member devices.</td>
</tr>
<tr>
<td><code>activity</code></td>
<td>Optional. Displays Smart RF activity related information Use this option to view the following:</td>
</tr>
<tr>
<td></td>
<td>• Time-period – Lists the frequency Smart RF activity is trended for the RF Domain. Trending periods include the current hour, last 24 hours, or the last seven days. Comparing Smart RF adjustments versus the last seven days enables an administrator to assess whether periods of interference and poor performance were relegated to just specific periods.</td>
</tr>
<tr>
<td></td>
<td>• Power changes – Displays the number of Smart RF initiated power level changes needed for RF Domain member devices during each of the three trending periods. Determine whether power compensations were relegated to known device outages or if compensations were consistent over the course of a day or week.</td>
</tr>
<tr>
<td></td>
<td>• Channel changes – Lists the number of Smart RF initiated channel changes needed for RF Domain member devices during each of the three trending periods. Determine if channel adjustments were relegated to known device count increases or decreases over the course of a day or week.</td>
</tr>
<tr>
<td></td>
<td>• Coverage changes – Displays the number of Smart RF initiated coverage changes needed for RF Domain member devices during each of the three trending periods. Determine if coverage changes were relegated to known device failures or known periods of interference over the course of a day or week.</td>
</tr>
<tr>
<td><code>energy</code></td>
<td>Optional. Displays AP energy for a specified AP or all APs Use this option to view an RF Domain member access point’s operating channels, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing access points.</td>
</tr>
<tr>
<td><code>neighbors</code></td>
<td>Optional. Displays AP neighbors Use this option to view attributes of neighbor radio resources available for Smart RF radio compensations for other RF Domain member device radios.</td>
</tr>
<tr>
<td>`{&lt;MAC&gt;</td>
<td>&lt;DEVICE-NAME&gt;}`</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;MAC&gt;</code> – Displays all of the above mentioned information for a specified AP, identified by its MAC address. Specify the AP’s MAC address.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-NAME&gt;</code> – Displays all of the above mentioned information for a specified AP, identified by its hostname. Specify the AP’s hostname.</td>
</tr>
<tr>
<td><code>on &lt;DOMAIN-NAME&gt;</code></td>
<td>Optional. Displays access point details on a specified RF Domain</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DOMAIN-NAME&gt;</code> – Specify the domain name.</td>
</tr>
</tbody>
</table>
### SHOW COMMANDS

#### history-timeline
Displays extended Smart RF calibration history on an hourly or daily timeline
Use this option to view the time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain.

<table>
<thead>
<tr>
<th>on &lt;DOMAIN-NAME&gt;</th>
<th>The following keyword is common to all of the above parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• on &lt;DOMAIN-NAME&gt; – Optional. Displays Smart RF configuration, based on the parameters passed, on a specified RF Domain</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</td>
</tr>
</tbody>
</table>

- `show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}`

#### smart-rf
Displays Smart RF related information

#### radio
Displays radio related commands

- `<MAC>` Optional. Displays details of a specified radio. Specify the radio’s MAC address in the AA-BB-CC-DD-EE-FF format.
- `all-11an` Optional. Displays all 11a radios currently in the configuration
- `all-11bgn` Optional. Displays all 11bg radios currently in the configuration

- `energy {<MAC>}` Optional. Displays radio energy
  - `<MAC>` – Optional. Specify the radio’s MAC address in the AA-BB-CC-DD-EE-FF format.
  - Use this option to view an RF Domain member access point radio’s operating channel, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.

- `on <DOMAIN-NAME>` The following keyword is common to all of the above parameters:
  - `on <DOMAIN-NAME>` – Optional. Displays radio details on a specified RF Domain
  - `<DOMAIN-NAME>` – Specify the RF Domain name.

- `show smart-rf radio {activity|neighbors} {<MAC>|all-11an|all-11bgn} {on <DOMAIN-NAME>}`

#### smart-rf
Displays Smart RF related information

#### radio
Displays Smart RF radio related commands

- `activity` Optional. Displays changes related to radio power, number of radio channels, or coverage holes. Use additional filters to view specific details.
- `<MAC>` Optional. Displays radio activity for a specified radio
  - `<MAC>` – Specify the radio’s MAC address.
- `all-11an` Optional. Displays radio activity of all 11a radios in the configuration
- `all-11bgn` Optional. Displays radio activity of all 11bg radios in the configuration

- `on <DOMAIN-NAME>` Optional. Displays radio activity of all radios within a specified RF Domain
  - `<DOMAIN-NAME>` – Specify the RF Domain name.

- `show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}`

#### smart-rf
Displays Smart RF related information

#### interfering-ap
Displays interfering access points (requiring potential isolation) information
show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>|threshold <50-100>}

smart-rf Displays Smart RF related information
interfering-ap Displays interfering neighboring access point information

<MAC> Optional. Displays interfering neighboring access point information
• <MAC> – Specify the access point’s MAC address.

Note: Considers all APs if this parameter is omitted

<DEVICE-NAME> Optional. Displays interfering neighboring access point information on a specified device
• <DEVICE-NAME> – Specify the device name.

Note: Considers all APs if this parameter is omitted

on <DOMAIN-NAME> Optional. Displays all interfering neighboring access point information within a specified RF Domain
• <DOMAIN-NAME> – Specify the RF Domain name.

threshold <50-100> Optional. Specifies the maximum attenuation threshold of interfering neighbors.
• <50-100> – Specify a value from 50 -100 dB.
Attenuation is a measure of the reduction of signal strength during transmission. Attenuation is the opposite of amplification, and is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible. Attenuation is measured in decibels.

on <DOMAIN-NAME> Optional. Displays radio activity of all radios within a specified RF Domain
• <DOMAIN-NAME> – Specify the RF Domain name.

Examples
rfs7000-37FABE(config)#show smart-rf calibration-status
No calibration currently in progress
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show smart-rf history
---------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>TIME</th>
<th>EVENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
---------------------------------------------------------------------------------------
|      |       |             |
---------------------------------------------------------------------------------------
Total number of history entries displayed: 0
rfs7000-37FABE(config)#
6.1.62 spanning-tree

Displays spanning tree utilization information

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

show spanning-tree mst {configuration|detail|instance|on <DEVICE-NAME>}
show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}
show spanning-tree mst {detail} {interface|on}
show spanning-tree mst {detail} interface {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}
show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>} {(on <DEVICE-NAME>)}

Parameters

- show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>spanning-tree</th>
<th>Displays spanning tree utilization information</th>
</tr>
</thead>
<tbody>
<tr>
<td>mst</td>
<td>Displays Multiple Spanning Tree (MST) related information</td>
</tr>
<tr>
<td>configuration</td>
<td>Optional. Displays MST configuration</td>
</tr>
<tr>
<td>{on &lt;DEVICE-NAME&gt;}</td>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Displays MST configuration on a specified device</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-NAME&gt; – Specify the name of the AP or wireless controller.</td>
</tr>
<tr>
<td></td>
<td>Note: If the 'on' keyword is used without any of the other options, the system displays a summary of spanning tree utilization information on the specified device.</td>
</tr>
</tbody>
</table>

- show spanning-tree mst {detail} interface {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>spanning-tree</th>
<th>Displays spanning tree information</th>
</tr>
</thead>
<tbody>
<tr>
<td>mst</td>
<td>Displays MST configuration</td>
</tr>
<tr>
<td>detail</td>
<td>Optional. Displays detailed MST configuration, based on the parameters passed</td>
</tr>
<tr>
<td>interface</td>
<td>Displays detailed MST configuration for a specified interface</td>
</tr>
<tr>
<td>[&lt;INTERFACE&gt;</td>
<td>ge &lt;1-4&gt;</td>
</tr>
<tr>
<td></td>
<td>- ge &lt;1-4&gt; – Displays GigabitEthernet interface MST configuration</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-4&gt; – Select the GigabitEthernet interface index from 1 - 4.</td>
</tr>
<tr>
<td></td>
<td>Note: The GE interface range for NX45XX and NX65XX service platforms is &lt;1 - 24&gt;</td>
</tr>
<tr>
<td></td>
<td>- me1 – Displays FastEthernet interface MST configuration</td>
</tr>
</tbody>
</table>

Contd..
**show spanning-tree mst**

{instance <1-15>} {interface <INTERFACE-NAME>}

**on <DEVICE-NAME>**

The following keyword is common to all interfaces:

- on <DEVICE-NAME> – Optional. Displays detailed MST configuration on a specified device
- <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
• show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>}
{on <DEVICE-NAME>)}
```

---

**spanning-tree**

Displays spanning tree information

**mst**

Displays MST configuration. Use additional filters to view specific details.

**instance <1-15>**

Optional. Displays information for a particular MST instance

- <1-15> – Specify the instance ID from 1 - 15.

**interface <INTERFACE-NAME>**

Optional. Displays MST configuration for a specific interface instance. The options are:

- <INTERFACE-NAME> – Displays MST configuration for a specified interface. Specify the interface name.

**on <DEVICE-NAME>**

Optional. Displays MST configuration on a specified device

- <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

---

### Examples

**rfs7000-37FABE(config)#show spanning-tree mst configuration**

```
%%
% MSTP Configuration Information for bridge 1 :
%------------------------------------------------------
% Format Id          : 0
% Name                : My Name
% Revision Level      : 0
% Digest              : 0xac36177f50283cd4b83821d8ab26de62
%------------------------------------------------------
```

**rfs7000-37FABE(config)#show spanning-tree mst detail interface test**

```
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast bpdu-filter errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
```

**rfs7000-37FABE(config)#**
rfs7000-37FABE(config)#show spanning-tree mst detail
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0  - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
% 1: ge4: Port 2004 - Id 87d4 - Role Disabled - State Forwarding
% 1: ge4: Designated External Path Cost 0 - Internal Path Cost 0
% 1: ge4: Configured Path Cost 11520 - Add type Implicit - ref count 1
% 1: ge4: Designated Port Id 0 - CST Priority 128
% 1: ge4: ge4: CIST Root 0000000000000000
% 1: ge4: ge4: Regional Root 0000000000000000
% 1: ge4: ge4: Designated Bridge 0000000000000000
% 1: ge4: Message Age 0 - Max Age 0
% 1: ge4: CIST Hello Time 0 - Forward Delay 0
% 1: ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% 1: ge4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
--More--
rfs7000-37FABE(config)#
### 6.1.63 startup-config

#### Show commands

Displays complete startup configuration script

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show startup-config {include-factory}
```

**Parameters**

- `include-factory` — Optional. Includes factory defaults

**Examples**

```
nx4500-5CFA2B# show startup-config

! Configuration of NX4500 version 5.8.1.0-037B
!
version 2.3
!
url-list AllowedShopping
    id 101
    url ebay.com depth 10
    url amazon.com depth 10
!
url-filter WebFilter_ShopingSites
    whitelist url-list AllowedShopping precedence 2 description description
    blacklist category-type news-sports-general category shopping precedence 1 description description
!
firewall-policy default
    no ip dos tcp-sequence-past-window
    alg sip
!
mint-policy global-default
--More--
nx4500-5CFA2B#
```
6.1.64 t5

Show commands
Displays adopted T5 controller statistics
Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7510, NX7520, NX9000,
  NX9500, NX9510, NX9600

NOTE: This command is applicable only on WiNG controllers with adopted and managed T5 controllers.

Syntax
show t5 [boot|clock|cpe|interface|mac|system|temperature|uptime|version|wireless] {on <DEVICE-NAME>}

Parameters
- show t5 [boot|clock|cpe|interface|mac|system|temperature|uptime|version|wireless] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>t5</th>
<th>Displays adopted T5 controller statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>Displays the T5 device’s boot details. Use this option to view the primary and secondary image files available to use for booting up.</td>
</tr>
<tr>
<td>clock</td>
<td>Displays the T5 controller’s system time, as reported from the controller itself or its remote NTP time resource</td>
</tr>
<tr>
<td>cpe</td>
<td>Displays the following details for T5 controller managed CPEs:</td>
</tr>
<tr>
<td></td>
<td>• address – Displays each CPE’s current IP address used as its network identifier</td>
</tr>
<tr>
<td></td>
<td>• boot – Displays the primary and secondary firmware versions available to each CPE, along with status of the most recent upgrade operation.</td>
</tr>
<tr>
<td></td>
<td>• ether port status – Displays Ethernet port status</td>
</tr>
<tr>
<td></td>
<td>• led – Displays whether the CPEs currently have their LEDs enabled or disabled. In places like hospitals, its not uncommon for access points to be operational, but their LEDs off as to not disturb patients.</td>
</tr>
<tr>
<td></td>
<td>• reset – Displays the number times a CPE has been reset</td>
</tr>
<tr>
<td></td>
<td>• system – Displays device hardware and SKU information for each CPE. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available.</td>
</tr>
<tr>
<td></td>
<td>• uptime – Displays the time each CPE device has been actively deployed and operational</td>
</tr>
<tr>
<td></td>
<td>• version – Displays the application and boot versions utilized by the CPE devices</td>
</tr>
</tbody>
</table>

Note: Use this screen to verify each CPE address credentials and whether currently disconnected or ready for radio coverage area support.
interface Displays T5 interface-related statistics. The interface options are:
- dsl – Displays DSL interface related information
- fe – Displays FE interface related information
- ge – Displays GE interface related information
- radio – Displays radio interface related information
The system displays the following information for the DSL, GE, and FE ports:
- counters – Displays the following:
  - Number of octets (bytes) received and transmitted on this port
  - Number of data packets received and transmitted on this port
  - Number of flow control (layer 2) packets received and transmitted on this port
- description – Displays the following:
  - The selected port’s name
  - The numeric index assignable to each port
  - The 64 character maximum, unique, administrator-assigned description to each port
- status – Displays the following:
  - The selected port’s name
  - Whether the port is currently up or down as a T5 controller transmit and receive resource
  - The port’s current speed in MB
  - Whether pause packet utilization is currently off or on for the port
  - Whether each listed port is enabled or disabled by the administrator
- utilization – Displays the following:
  - The selected port’s name
  - The port’s receive and transmit data rates (in Kbps)
  - A packet per second port receive and transmit rate (p/s)
  - Each port’s receive and transmit direction utilization as a percentage of transmit bandwidth available
The system displays the following information specific to the DSL port:
- custom – Displays the following DSL-related data:
  - Lists each DSL’s average response time in microseconds.
  - Lists each DSL’s maximum (best to date since last refresh) response time in microseconds.
  - Lists the number of seconds downstream DSL transmissions were negatively impacted by code violations.
  - Lists the number of seconds downstream DSL transmissions were severely negatively impacted by code violations.
  - Lists the number of seconds upstream DSL transmissions were negatively impacted by code violations.
  - Lists the number of seconds upstream DSL transmissions were severely negatively impacted by code violations.
• **errors** – Displays the following DSL-related errors:
  - The name of the DSL utilized by each T5 controller connected CPE device.
  - The number of Fecs detected in the downstream direction. *Forward Error Correction* (FEC) or channel coding is used for controlling errors over unreliable or noisy communication channels.
  - The number of CPE DSL coding violations (badly coded packets) detected in the downstream direction.
  - The number of Fecs detected in the upstream direction.
  - The number of CPE DSL coding violations (badly coded packets) detected in the upstream direction.

The system displays the following information for each listed **radio** interface:

• **status** – Displays the following:
  - Administrator assigned name of each listed CPE radio as its unique identifier.
  - Whether the selected radio is currently up or down in its ability to be a radio coverage resource for its managing T5 controller.
  - The factory encoded MAC address.
  - The configured transmit power.
  - The current transmit channel.

• **statistics** – Displays the following:
  - The radio's receive and transmit data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.
  - The number of octets (bytes) received and transmitted with no errors by the CPE radio.
  - The number of data packets received or transmitted by the CPE radio.

• **WLAN map** – Displays the following:
  - The managed WLAN(s) to which each listed radio has been mapped.

| **mac** | Displays T5 MAC address table. Use the additional filters to filter on the basis of the VLAN or DSL interface. |
| **system** | Displays T5 controller’s system information, which includes the T5 controller’s hostname, MAC address, RF Domain, system clock, uptime. |
| **temperature** | Displays T5 controller’s current temperature. |
| **uptime** | Displays the T5 controller’s uptime (the time it has been actively deployed and operational). |
| **version** | Displays the T5 controller’s primary and secondary firmware images. |
**Examples**

The following examples are for show commands executed on the 't5-ED5EE8' controller adopted by the 'rfs7000-37FABE' wireless controller:

```
rfs7000-37FABE#show t5 boot on t5-ED5EE8
Primary Version: 5.3.2.88-015R
Secondary Version: 5.3.2.88-011B
Next Boot: Primary
Upgrade Status: none
Upgrade Progress %: 0
rfs7000-37FABE#
```

```
rfs7000-37FABE#show t5 version on t5-ED5EE8
Bootloader Version: 5.0.0.0-070R
Application Version: 5.3.2.88-015R
rfs7000-37FABE#
```

```
rfs7000-37FABE#show t5 system on t5-ED5EE8
Serial Number 13322522400053
SKU TS-0524-WR
Hardware Rev 5
Mac Address B4:C7:99:ED:5E:E8
Description 24-port PowerBroadband VDSL2 Switch Version 5.3.2.88-015R
Contact NULL
Name t5-ED5EE8
Location NULL
rfs7000-37FABE#
```

```
rfs7000-37FABE#show t5 clock on t5-ED5EE8
Time 22-5-2015 23:25:1 UTC
rfs7000-37FABE#
```
rfs7000-37FABE#show t5 interface ge counter on t5-ED5EE8

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>RX OCTETS</th>
<th>RX PACKETS</th>
<th>RX PAUSE</th>
<th>PKTS</th>
<th>TX OCTETS</th>
<th>TX PACKETS</th>
<th>TX PAUSE</th>
<th>PKTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge1</td>
<td>21...496</td>
<td>1074917</td>
<td>0</td>
<td>87957721</td>
<td>498090</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#

rfs7000-37FABE#show t5 uptime on t5-ED5EE8
Up Time 6 days 23:50:08
rfs7000-37FABE#

rfs7000-37FABE#show t5 temperature on t5-ED5EE8
============ Temperature ============
<table>
<thead>
<tr>
<th>INDEX</th>
<th>CURRENT (C)</th>
<th>FANS @ FULL SPEED (C)</th>
<th>FANS @ VARIABLE SPEED (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>41</td>
<td>70</td>
<td>60</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#

rfs7000-37FABE#show t5 cpe address on t5-ED5EE8

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>STATUS</th>
<th>IP ADDRESS</th>
<th>MAC ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpe1</td>
<td>disconnected</td>
<td>0.0.0.0</td>
<td>00:00:00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>cpe2</td>
<td>disconnected</td>
<td>0.0.0.0</td>
<td>00:00:00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>cpe3</td>
<td>disconnected</td>
<td>0.0.0.0</td>
<td>00:00:00:00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

--More--

rfs7000-37FABE#

rfs7000-37FABE#show t5 cpe led on t5-ED5EE8

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>LED STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpe1</td>
<td>enable</td>
</tr>
<tr>
<td>cpe2</td>
<td>enable</td>
</tr>
<tr>
<td>cpe3</td>
<td>enable</td>
</tr>
<tr>
<td>cpe4</td>
<td>enable</td>
</tr>
<tr>
<td>cpe5</td>
<td>enable</td>
</tr>
<tr>
<td>cpe6</td>
<td>enable</td>
</tr>
<tr>
<td>cpe7</td>
<td>enable</td>
</tr>
<tr>
<td>cpe8</td>
<td>enable</td>
</tr>
<tr>
<td>cpe9</td>
<td>enable</td>
</tr>
<tr>
<td>cpe10</td>
<td>enable</td>
</tr>
<tr>
<td>cpe11</td>
<td>enable</td>
</tr>
<tr>
<td>cpe12</td>
<td>enable</td>
</tr>
<tr>
<td>cpe13</td>
<td>enable</td>
</tr>
<tr>
<td>cpe14</td>
<td>enable</td>
</tr>
<tr>
<td>cpe15</td>
<td>enable</td>
</tr>
<tr>
<td>cpe16</td>
<td>enable</td>
</tr>
<tr>
<td>cpe17</td>
<td>enable</td>
</tr>
<tr>
<td>cpe18</td>
<td>enable</td>
</tr>
<tr>
<td>cpe19</td>
<td>enable</td>
</tr>
<tr>
<td>cpe20</td>
<td>enable</td>
</tr>
<tr>
<td>cpe21</td>
<td>enable</td>
</tr>
<tr>
<td>cpe22</td>
<td>enable</td>
</tr>
<tr>
<td>cpe23</td>
<td>enable</td>
</tr>
<tr>
<td>cpe24</td>
<td>enable</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#
nx9500-6C8809#show t5 mac table filter name vlan 1 on t5-ED5EAC

<table>
<thead>
<tr>
<th>T5-MAC</th>
<th>VLAN</th>
<th>ADDRESS</th>
<th>INTERFACE</th>
<th>VENDOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-04-96-43-4C-AA</td>
<td>ge1</td>
<td>Extreme Networks</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-23-68-11-E6-C4</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-23-68-88-0D-A7</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-23-68-88-0D-A8</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-23-68-99-BB-7C</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-23-68-99-BB-7D</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>00-A0-F8-68-D5-67</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>3C-CE-73-F4-47-83</td>
<td>ge1</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>5C-0E-8B-18-10-91</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>5C-0E-8B-18-10-92</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>B4-C7-99-5C-FA-2B</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>B4-C7-99-5C-FA-8E</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>B4-C7-99-5C-FA-8F</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>B4-C7-99-6C-8B-09</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>B4-C7-99-74-B4-5C</td>
<td>ge1</td>
<td>Zebra Tech</td>
</tr>
<tr>
<td>B4-C7-99-ED-5E-AC</td>
<td>1</td>
<td>B4-C7-99-ED-5E-AC</td>
<td>co</td>
<td>Zebra Tech</td>
</tr>
</tbody>
</table>

--More--

nx9500-6C8809#
### 6.1.65 terminal

- **show commands**

Displays terminal configuration parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show terminal`

**Parameters**

None

**Examples**

```
show terminal
Terminal Type: xterm
Length: 24    Width: 200
```

```
rfs7000-37FABE(config)#show terminal
```
6.1.66 timezone

- **show commands**
  Displays a device’s timezone

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show timezone`

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config)#show timezone
Timezone is America/Los_Angeles
rfs7000-37FABE(config)#
```
### 6.1.67 traffic-shape

> **show commands**

Displays traffic-shaping related configuration details and statistics.

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target’s interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, ACL rules take precedence for the traffic shaping class. Using traffic shaping, an application takes precedence over an application category.

Supported in the following platforms:

- Access Points — AP622, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530

#### Syntax

```
show traffic-shape [priority-map|statistics {class <1-4>}|status] {on <DEVICE-NAME>}
```

#### Parameters

- **show traffic-shape [priority-map|statistics {class <1-4>}|status] {on <DEVICE-NAME>}**

<table>
<thead>
<tr>
<th>traffic-shape</th>
<th>Displays traffic-shaping related configuration details and statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-map</td>
<td>Displays the traffic shaper queue priority. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets 802.1p markings.</td>
</tr>
<tr>
<td>statistics class &lt;1-4&gt;</td>
<td>Displays traffic-shaping related statistics for all traffic shaper classes or for a selected class</td>
</tr>
<tr>
<td>status</td>
<td>Displays the controller or service platform’s traffic shaping status (whether running or not)</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays traffic-shaping related configuration details and statistics on a specified device</td>
</tr>
</tbody>
</table>

#### Examples

```
ap7532-DEB9B0#show traffic-shape priority-map
----------------------------------------------------------
DOT1P-PRIORITY   TX-SHAPER-PRIORITY
0                2
1                0
2                1
3                3
4                4
5                5
6                6
7                7
----------------------------------------------------------
ap7532-DEB9B0#
```
ap7532-DEB9B0# show traffic-shape status
State of Traffic shaper: running
ap7532-DEB9B0#

ap7532-DEB9B0# show traffic-shape statistics

Traffic shaper class : 1
Class 1 is not configured:

Traffic shaper class : 3
Class 3 is not configured:

Traffic shaper class : 2
Rate: 1500 Kbps

<table>
<thead>
<tr>
<th>PRIORITY</th>
<th>PKTS-SENT</th>
<th>PKTS-DELAYED</th>
<th>PKTS-DROPPED</th>
<th>CURRENT-QUEUE-LEN</th>
<th>CURRENT-LATENCY (IN USECS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>152153035</td>
<td>151924251</td>
<td>1508343</td>
<td>11</td>
<td>33447</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Traffic shaper class : 4
Class 4 is not configured:

ap7532-DEB9B0#
### 6.1.68 upgrade-status

<table>
<thead>
<tr>
<th>show commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the last image upgrade status</td>
</tr>
</tbody>
</table>

**NOTE:** This command is not available in the USER EXEC Mode.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show upgrade-status {detail|on}
show upgrade-status {detail} {(on <DEVICE-NAME>)}
```

**Parameters**

- `show upgrade-status {detail|on}`
- `on <DEVICE-NAME>`

<table>
<thead>
<tr>
<th>upgrade-status</th>
<th>Displays last image upgrade status and log</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Optional. Displays last image upgrade status in detail</td>
</tr>
</tbody>
</table>

- The following keyword is recursive and common to the `detail` parameter:
  - `on <DEVICE-NAME>` – Optional. Displays last image upgrade status on a specified device
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

**Note:** If the `on` keyword is used without the `detail` keyword, the system displays a summary of upgrade status and log on the specified device.

**Examples**

```
rfs4000-229D58# show upgrade-status
Last Image Upgrade Status: In_Progress (3 percent completed)
Last Image Upgrade Time: 2015-06-08 08:37:45
rfs4000-229D58#
```

```
rfs4000-229D58# show upgrade-status
Last Image Upgrade Status: Successful
Last Image Upgrade Time: 2015-06-08 08:45:54
rfs4000-229D58#
```

```
rfs4000-229D58(config)# show upgrade-status detail
Last Image Upgrade Status: Successful
Last Image Upgrade Time: 2015-06-08 08:45:54
-----------------------------------------------
Running from partition /dev/mtdblock6
var2 is 3 percent full
/tmp is 3 percent full
Free Memory 97176 kB
FWU invoked via Linux shell
Validating image file header
Making file system
Extracting files (this may take some time).
Control C disabled
Version of firmware update file is 5.8.1.0-037B
rfs4000-229D58#```
Writing Kernel to /dev/mtd5
Writing BootOS to /dev/mtd3
Successful

rfs4000-229D58(config)#
6.1.69 version

> show commands

Displays a device’s software and hardware version

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
show version {on <DEVICE-NAME>}
```

Parameters

- `show version {on <DEVICE-NAME>}`

| version {on <DEVICE-NAME>} | Displays software and hardware versions on all devices or a specified device  
- on <DEVICE-NAME> – Optional. Displays software and hardware versions on a specified device  
- <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

Examples

```
rfs4000-229D58(config)#show version
RFS4000 version 5.8.1.0-037B
Copyright (c) 2004-2015 Symbol Technologies, Inc. All rights reserved.
Booted from secondary

rfs4000-229D58 uptime is 3 days, 03 hours 28 minutes
CPU is Cavium Networks Octeon CN50XX V0.1
Base ethernet MAC address is 00-23-68-22-9D-58
System serial number is 9184521800027
Model number is RFS-4010-00010-WR
PoE firmware version is 211 build 1
FPGA version is 2.26
Radio HAL version is 92 (DFS:73)
```

```
rfs4000-229D58(config)#
```
### 6.1.70 vrrp

**show commands**

Displays the following Virtual Router Redundancy Protocol (VRRP) related statistics: configuration error, router redundancy information in brief and detail. VRRP configuration errors include mismatch of authentication credentials, invalid packet checksums, invalid packet types, invalid virtual route IDs, TTL errors, packet length errors and invalid (non matching) VRRP versions.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}
show vrrp error-stats {on <DEVICE-NAME>}
```

**Parameters**

- **vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}**
  - **brief** Displays VRRP related statistics in brief or in detail depending on the option selected.
  - **details** Displays virtual router information in brief.
  - **stats** Displays virtual router information in detail.
  - **<1-255>** The following keyword is common to all of the above parameters:
    - **<1-255>** – Optional. Displays information for a specified Virtual Router. Specify the router's ID from 1 - 255.
  - **on <DEVICE-NAME>** The following keyword is recursive and common to the '<1-255>' parameter:
    - **on <DEVICE-NAME>** – Optional. Displays specified router information on a specified device.
    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

- **show vrrp error-stats {on <DEVICE-NAME>**

```
error-stats {on <DEVICE-NAME>}
```

- **error-stats {on <DEVICE-NAME>**
  - **error-stats** Displays VRRP related statistics in brief or in detail depending on the option selected.
  - **on <DEVICE-NAME>** Displays global error statistics:
    - **on <DEVICE-NAME>** – Optional. Displays global error statistics on a specified device.
    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.
**Examples**

```plaintext
rfs7000-37FABE(config)#show vrrp error-stats
Last protocol error reason: none
IP TTL errors: 0
Version mismatch: 0
Packet Length error: 0
Checksum error: 0
Invalid virtual router id: 0
Authentication mismatch: 0
Invalid packet type: 0
rfs7000-37FABE(config)#
```

```plaintext
rfs7000-37FABE(config)#show vrrp details
VRRP Group 1:
  version 2
  interface none
  configured priority 1
  advertisement interval 1 sec
  preempt enable, preempt-delay 0
  virtual mac address 00-00-5E-00-01-01
  sync group disable
rfs7000-37FABE(config)#
```
### 6.1.71 web-filter

* show commands

Displays Web filtering related information

Use this command to view information on Web requests for content and whether the requests were blocked or approved based on URL filter settings defined for the selected controller or service platform. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP7131, AP7502, AP7522, AP7532, AP7562, AP8132
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
show web-filter [category|category-type|config|filter-level [basic|high|low|medium|medium-high]|statistics {on <DEVICE-NAME>}|status]
```

**Parameters**

- `show web-filter [category|category-type|config|filter-level [basic|high|low|medium|medium-high]|statistics {on <DEVICE-NAME>}|status]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-filter</td>
<td>Displays an existing and configured Web filter details</td>
</tr>
<tr>
<td>category</td>
<td>Displays Web filter categories. A category is a pre-defined URL list available in the WiNG software.</td>
</tr>
<tr>
<td>category-type</td>
<td>Displays the Web filter category types. This is a pre-configured list of categories and sub-categories in which commonly accessed URLs have been classified.</td>
</tr>
<tr>
<td>config</td>
<td>Displays all existing Web filters and their configuration details</td>
</tr>
<tr>
<td>filter-level [basic</td>
<td>high</td>
</tr>
<tr>
<td>statistics {on &lt;DEVICE-NAME&gt;}</td>
<td>Displays Web filter statistics on a specified device</td>
</tr>
<tr>
<td>status {on &lt;DEVICE-NAME&gt;}</td>
<td>Displays Web filter status on a specified device</td>
</tr>
</tbody>
</table>

**Note:** Web filtering is a licensed feature, and only when enforced can the system display Web filtering statistics.
Examples

```
nx9500-6C8809(config)#show web-filter category
    advertisement-popups
        Sites that provide advertising graphics or other ad content files such as banners and pop-ups.
    alcohol-tobacco
        Sites that promote or sell alcohol- or tobacco-related products or services.
    anonymizers
        Sites and proxies that act as an intermediary for surfing to other websites in an anonymous fashion, whether to circumvent web filtering or for other reasons.
    arts
        Sites with artistic content or relating to artistic institutions such as theaters, museums, galleries, dance companies, photography, and digital graphic resources.
    botnets
        Sites that use bots (zombies) including command-and-control sites.
--More--
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show web-filter config
URL filters configured for this device are:
    WebFilter_ShoppingSites
        Blacklisted categories:
            shopping,
        Whitelisted categories:
            <AllowedShopping>,
nx9500-6C8809(config)#
```
### 6.1.72 what

**show commands**

Displays details of a specified search phrase (performs global search)

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contain &lt;WORD&gt;</td>
<td>Searches on all the items that contain a specified word</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify a word to search (for example, MAC address, hostname etc.)</td>
</tr>
<tr>
<td>is &lt;WORD&gt;</td>
<td>Searches on an exact match</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify a word to search (for example, MAC address, hostname etc.)</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Performs global search on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller,</td>
</tr>
<tr>
<td></td>
<td>service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58#show what contain default
---------------------------------------------------------------------------------------
NO. CATEGORY             MATCHED                        OTHER KEY INFO (1)             OTHER KEY INFO (2)             OTHER KEY INFO (3)             OTHER
NAME/VALUE                     NAME/VALUE                     NAME/VALUE                     NAME/VALUE                     NAME/VALUE
---------------------------------------------------------------------------------------
rf_domain_name
1   device-cfg           default-trustpoint             rfs4000                        00-23-68-22-9D-58              default
2   firewall_policy      default                        default                        name                           https
3   management_policy    default                        default                        True                           30
bezcon_format
--More--
rfs4000-229D58#
```
6.1.73 wireless

- **show commands**
  Displays wireless configuration parameters

Supported in the following platforms:
- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```bash
show wireless [ap|bridge|client|meshpoint|mobility-database|radio|regulatory|rf-domain|sensor-server|unsanctioned|wips|wlan]

show wireless ap {configured|detail|load-balancing|on <DEVICE-NAME>}
show wireless ap {configured}
show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless ap {load-balancing} {client-capability|events|neighbors} {(on <DEVICE-NAME>)}

show wireless bridge {candidate-ap|certificate|config|hosts|on|statistics}
show wireless bridge {candidate-ap} {<MAC/HOSTNAME> {1-3}} {(filter radio-mac <RADIO-MAC>) {(on <DEVICE-OR-DOMAIN-NAME>)}}
show wireless bridge {certificate} status {(on <DEVICE-NAME>)}
show wireless bridge {config}
show wireless bridge {hosts} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless bridge {statistics} {rf|traffic} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless client {association-history|detail|filter|include-ipv6|on <DEVICE-OR-DOMAIN-NAME>|statistics|tspec}
show wireless client {association-history <MAC}> {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {detail <MAC}> {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {filter [ip|on|state|wlan]} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {ip [{IP}|not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {state [data-ready|not [data-ready|roaming]|roaming]} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {wlan [<WLAN-NAME]|not <WLAN-NAME>]} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {include-ipv6} {detail|on|filter}
show wireless client {include-ipv6} {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {include-ipv6} {filter {ip|ipv6|state|wlan}} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {statistics} {detail|on|rf>window-data}
show wireless client {statistics} {detail <MAC>|rf>window-data <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {tspec <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

show wireless meshpoint {config|detail|multicast|neighbor|on|path|proxy|root|security|statistics|tree|usage-mappings}
show wireless meshpoint {config} {filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}}
show wireless meshpoint {detail} {<MESHPOINT-NAME>}
show wireless meshpoint {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {multicast|path|proxy|root|security|statistics} [<MESHPOINT-NAME>]{detail} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint neighbor [<MESHPOINT-NAME>]{detail|statistics} {rf} {on <DEVICE-OR-DOMAIN-NAME>}
```
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {usage-mappings}

show wireless mobility-database {on <DEVICE-NAME>}

show wireless radio {detail|on <DEVICE-OR-DOMAIN-NAME>|statistics|tspec|wlan-map}
show wireless radio {detail} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio {detail} {<DEVICE-NAME> {<1-3>|filter|on}}
show wireless radio {filter <RADIO-MAC>} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio {statistics} {detail|on|rf|windows-data} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless rf-domain statistics {detail} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless sensor-server {on <DEVICE-OR-DOMAIN-NAME>}
show wireless unsanctioned aps {detail|statistics} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless wips {client-blacklist|event-history} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless wlan {config|detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|statistics|usage-mappings}
show wireless wlan {config|detail <WLAN>} {on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|usage-mappings}
show wireless wlan {config filter {device <DEVICE-NAME> rf-domain <DOMAIN-NAME>}}
show wireless wlan {statistics <WLAN>}{detail|traffic} {on <DEVICE-OR-DOMAIN-NAME>}

Parameters

- show wireless ap {configured}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>Displays managed access point information</td>
</tr>
<tr>
<td>configured</td>
<td>Optional. Displays configured AP information, such as name, MAC address, profile, RF Domain and adoption status</td>
</tr>
</tbody>
</table>

- show wireless ap {detail} {<MAC/HOST-NAME>} {on <DEVICE-OR-DOMAIN-NAME>}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>Displays managed access point information</td>
</tr>
<tr>
<td>detail &lt;MAC/HOST-NAME&gt;</td>
<td>Optional. Displays detailed information for all APs or a specified AP</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is recursive and common to the ‘detail &lt;MAC/HOST-NAME&gt;’ parameter:</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Displays information on a specified device or RF Domain</td>
</tr>
<tr>
<td>&lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>
### Command Overview

- **show wireless ap**
  - `load-balancing` {client-capability|events|neighbors}
  - `{on <DEVICE-NAME>}`
  - Displays wireless configuration parameters.
  - Displays managed access point information.

- **show wireless bridge**
  - `candidate-ap` {<MAC/HOSTNAME> {<1-3>}}
  - `{filter radio-mac <RADIO-MAC>}`
  - `{on <DEVICE-OR-DOMAIN-NAME>}`
  - Optional. Displays information about the candidate infrastructure access points as well as the infrastructure access point that the client-bridge radio has selected.
  - Note: When enabled, the client-bridge radio scans its defined channels to locate the best candidate access point servicing the infrastructure WLAN.

- **show wireless bridge certificate status** `{on <DEVICE-NAME>}`
  - Displays all client bridges in configuration and the status of their PKCS#12 certificates.
  - Optional. Executes the command on a specified device or devices within a specified RF Domain.
  - `on <DEVICE-OR-DOMAIN-NAME>` – Specify the AP, controller, service platform, or Domain name.

### Command Details

- **load-balancing**
  - `client-capability|events|neighbors` Optional. Displays load balancing status. Use additional filters to view specific details.
    - `events` – Optional. Displays client events.
    - `neighbors` – Optional. Displays neighboring clients.

- **on <DEVICE-NAME>**
  - The following keyword is recursive and common to the ‘client-capability’, ‘events’, and ‘neighbors’ parameters.
    - `on <DEVICE-NAME>` – Optional. Displays load balancing information, based on the parameters passed, on a specified device.
    - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

- **bridge candidate-ap**
  - Optional. Displays information about the candidate infrastructure access points as well as the infrastructure access point that the client-bridge radio has selected.

- **<MAC/HOSTNAME> <1-3>**
  - Optional. Specify the client-bridge access point’s hostname or MAC address. Optionally append the radio interface’s number to form client-bridge in the form of AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX.
  - `<1-3>` – Optional. Radio interface index if not specified as part of mesh ID.

- **filter radio-mac <RADIO-MAC>**
  - This is a recursive parameter and common to all of the above options.
  - `filter radio-mac` – Optional. Provides additional filters to specifically identify the radio by its MAC address.
  - `<RADIO-MAC>` – Specify the radio’s MAC address.

- **on <DEVICE-OR-DOMAIN-NAME>**
  - This is a recursive parameter and common to all of the above options.
  - `on <DEVICE-OR-DOMAIN-NAME>` – Optional. Executes the command on a specified device or devices within a specified RF Domain.
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the AP, controller, service platform, or Domain name.

### Additional Commands

- **show wireless bridge {certificate} status {on <DEVICE-NAME>]**
  - Displays wireless configuration statistics.

- **show wireless bridge {config}**
  - Displays wireless configuration statistics.
### bridge config
Optional. Displays all client bridges in configuration
The output displays the configured client-bridges’ hostname, MAC address, profile, RF Domain, SSID, band, encryption, authentication, and EAP username.

### show wireless bridge {hosts} {on <DEVICE-OR-DOMAIN-NAME>}

### wireless
Displays wireless configuration statistics

### bridge hosts
Optional. Displays the client bridge host information
The output displays the configured client-bridges’ host’s MAC Address, bridge MAC address, IPv4 address, bridging status, and activity
**Note:** The HOST MAC column displays real MAC addresses of wired hosts, while the BRIDGE MAC column displays the translated MAC addresses. The BRIDGE MAC column is based on the radio 2 base MAC address and increments by 1 for each wired host connected to the client bridges Ge1 port.

### on <DEVICE-OR-DOMAIN-NAME>
Optional. Executes the command on a specified device or devices within a specified RF Domain
• <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the AP, controller, service platform, or Domain name.

### show wireless bridge {statistics} {rf|traffic} {on <DEVICE-OR-DOMAIN-NAME>}

### wireless
Displays wireless configuration statistics

### bridge statistics
Optional. Displays the client-bridge related statistics

### rf
Optional. Displays the client-bridge related RF statistics
The output displays the signal, noise, SNR, TX/RX rates, retries, and errors.

### traffic
Optional. Displays the client-bridge related traffic statistics
The output displays TX/RX bytes, TX/RX packets, TX/RX bits/second, and dropped packets.

### on <DEVICE-OR-DOMAIN-NAME>
Optional. Executes the command on a specified device or devices within a specified RF Domain
• on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the AP, controller, service platform, or Domain name.

### show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

### wireless
Displays wireless configuration parameters

### client
Displays client information based on the parameters passed

### association-history <MAC>
Optional. Displays association history for a specified client
• <MAC> – Specify the MAC address of the client.

### on <DEVICE-OR-DOMAIN-NAME>
Optional. Displays association history on a specified device or RF Domain
• <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

### show wireless client {detail <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

### wireless
Displays wireless configuration parameters

### client
Displays client information based on the parameters passed
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless client</code></td>
<td>Displays client information based on the parameters passed.</td>
</tr>
<tr>
<td>`filter ip [&lt;IP&gt;</td>
<td>not &lt;IP&gt;]`</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>The following keyword is common to the ‘IP’ and ‘not IP’ parameters:</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays selected wireless client information on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless client</code></td>
<td>Displays client information based on the parameters passed.</td>
</tr>
<tr>
<td><code>filter state</code></td>
<td>Optional. Filters clients based on their state</td>
</tr>
<tr>
<td></td>
<td>- Roaming – Selects roaming clients</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>The following keyword is common to the ‘ready’, ‘not’, and ‘roaming’ parameters:</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays selected client details on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless client</code></td>
<td>Displays client information based on the parameters passed.</td>
</tr>
<tr>
<td><code>filter wlan</code></td>
<td>Optional. Filters clients on a specified WLAN</td>
</tr>
<tr>
<td>`[&lt;WLAN-NAME&gt;</td>
<td>not &lt;WLAN-NAME&gt;]`</td>
</tr>
<tr>
<td></td>
<td>- not &lt;WLAN-NAME&gt; – Inverts the match selection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail &lt;MAC&gt;</code></td>
<td>Optional. Displays detailed wireless client(s) information</td>
</tr>
<tr>
<td></td>
<td>- &lt;MAC&gt; – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.</td>
</tr>
</tbody>
</table>
The following keyword is common to the 'WLAN and 'not' parameters:
- on <DEVICE-OR-DOMAIN-NAME> – Optional. Filters clients on a specified device or RF Domain
  - <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- show wireless client {statistics} {detail <MAC>|rf|window-data <MAC>}
  {(on <DEVICE-OR-DOMAIN-NAME>)}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Displays client information based on the parameters passed</td>
</tr>
</tbody>
</table>

| statistics {detail <MAC>|rf|window-data <MAC>} | Optional. Displays detailed client statistics. Use additional filters to view specific details. |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------|
| detail <MAC> – Optional. Displays detailed client statistics |
| <MAC> – Optional. Displays detailed statistics for a specified client. Specify the client's MAC address. |
| rf – Optional. Displays detailed client statistics on a specified device or RF Domain |
| window-data <MAC> – Optional. Displays historical data, for a specified client |
| <MAC> – Optional. Specify the client's MAC address |

The following keyword is recursive and common to the 'detail <MAC>', 'RF', and 'window-data <MAC>' parameters:
- on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays client statistics, based on the parameters passed, on a specified device or RF Domain
  - <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- show wireless client {tspec} {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Displays client information based on the parameters passed</td>
</tr>
<tr>
<td>tspec &lt;MAC&gt;</td>
<td>Optional. Displays detailed traffic specification (TSPEC) information for all clients or a specified client</td>
</tr>
<tr>
<td>&lt;MAC&gt; – Optional. Displays detailed TSPEC information for a specified client. Specify the MAC address of the client.</td>
<td></td>
</tr>
</tbody>
</table>

on <DEVICE-OR-DOMAIN-NAME> The following keyword is recursive and common to the 'tspec <MAC>' parameter:
- on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed TSPEC information for wireless clients on a specified device or RF Domain
  - <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- show wireless client {include-ipv6} {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Displays client information based on the parameters passed</td>
</tr>
<tr>
<td>include-ipv6</td>
<td>Includes IPv6 address (if known) of wireless clients</td>
</tr>
<tr>
<td>detail &lt;MAC&gt;</td>
<td>Optional. Displays detailed wireless client(s) information</td>
</tr>
<tr>
<td>&lt;MAC&gt; – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.</td>
<td></td>
</tr>
</tbody>
</table>
on <DEVICE-OR-DOMAIN-NAME>  

The following keyword is recursive and common to the ‘detail <MAC>’ parameter:
- on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed information on a specified device or RF Domain
- <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

• show wireless client {include-ipv6} {filter {ip|ipv6|state|wlan}}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Displays wireless client information based on the parameters passed</td>
</tr>
</tbody>
</table>
| include-ipv6 {filter} | Optional. Includes IPv6 address (if known) of wireless clients  
  • filter – Optional. Defines additional filters. Use one of the following options to filter clients: ip, ipv6, state, and wlan  
  **Note:** By default the system only displays the IPv4 address of clients. The include-ipv6 parameter includes the known IPv6 address of each client. |
| ip [<IPv4>|not <IPv4>] | Optional. Displays wireless client information based on the IPv4 address passed  
  • <IPv4> – Displays information of the client identified by the <IPv4> parameter  
  • not <IPv4> – Inverts the match selection |
| ipv6 [<IPv6>|not <IPv6>] | Optional. Displays wireless client information based on the IPv6 address passed  
  • <IPv6> – Displays information of the client identified by the <IPv6> parameter  
  • not <IPv6> – Inverts the match selection |
| filter state [data-ready|not [data-ready|roaming]|roaming] | Optional. Filters wireless client information based on their state  
  • data-ready – Displays information of wireless clients in the data-ready state  
  • not [data-ready|roaming] – Inverts match selection. Displays information of wireless clients neither ready nor roaming  
  • Roaming – Displays information of roaming clients |
| wlan [<WLAN-NAME>|not <WLAN-NAME>] | Optional. Displays wireless client information based on the WLAN name passed  
  • <WLAN-NAME> – Specify the WLAN name.  
  • not <WLAN-NAME> – Inverts match selection |

• show wireless meshpoint {config} {filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}}

| wireless | Displays wireless configuration parameters. Use this option to view detailed statistics on each Mesh-capable client available within controller’s adopted access point’s radio coverage area.  
  A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| meshpoint | Displays meshpoint related information |
show wireless meshpoint
{detail} {<MESHPOINT-NAME>}

wireless
Displays wireless configuration parameters

meshpoint
Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller’s adopted access point’s radio coverage area.

A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes.

detail
{<MESHPOINT-NAME>}
Optional. Displays detailed information for all meshpoints or a specified meshpoint

• <MESHPOINT-NAME> – Optional. Displays detailed information for a specified meshpoint. Specify the meshpoint name.

show wireless meshpoint
{multicast|path|proxy|root|security|statistics}
[<MESHPOINT-NAME>|detail] {on <DEVICE-OR-DOMAIN-NAME>}

wireless
Displays wireless configuration parameters

meshpoint
Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller’s adopted access point’s radio coverage area.

A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes.

multicast
Optional. Displays meshpoint multicast information

path
Optional. Displays meshpoint path information

proxy
Optional. Displays meshpoint proxy information

root
Optional. Displays meshpoint root information

security
Optional. Displays meshpoint security information

statistics
Optional. Displays meshpoint statistics
### Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless meshpoint</code></td>
<td>Displays meshpoint related information. Use this option to view detailed statistics on each mesh-capable client available within controller’s adopted access point’s radio coverage area. A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes.</td>
</tr>
<tr>
<td><code>show wireless meshpoint {neighbor} [on &lt;DEVICE-OR-DOMAIN-NAME&gt;]</code></td>
<td>Optional. Displays meshpoint neighbor information, based on the parameters passed.</td>
</tr>
<tr>
<td><code>show wireless meshpoint {tree} [on &lt;DEVICE-OR-DOMAIN-NAME&gt;]</code></td>
<td>Optional. Displays meshpoint network tree on a specified device or RF Domain.</td>
</tr>
</tbody>
</table>

### Keywords

- **`<MESHPOINT-NAME>`** – Displays meshpoint related information for a specified meshpoint. Specify the meshpoint name.
- **`detail`** – Displays detailed multicast information for all meshpoints
- **`on <DEVICE-OR-DOMAIN-NAME>`** – Optional. Displays meshpoint neighbor information, based on the parameters passed, on a specified device or RF Domain. Specify the name of AP, wireless controller, service platform, or RF Domain.
- **`<DEVICE-OR-DOMAIN-NAME>`** – Specify the name of AP, wireless controller, service platform, or RF Domain.

**Note:**
The `show > wireless > meshpoint > tree` command can be executed only from a wireless controller.
### show wireless meshpoint

`{usage-mappings|on <DEVICE-OR-DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
</tr>
<tr>
<td>meshpoint</td>
<td>Displays meshpoint related information</td>
</tr>
<tr>
<td>usage-mappings</td>
<td>Optional. Lists all devices and profiles using the meshpoint</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Displays meshpoint applied to a specified device or RF Domain</td>
</tr>
</tbody>
</table>

- `<DEVICE-OR-DOMAIN-NAME>` – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain

### show wireless mobility-database

`{on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
</tr>
<tr>
<td>mobility-database</td>
<td>Displays controller-assisted mobility database</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is recursive and common to the ‘filter &lt;RADIO-MAC&gt;’ parameter:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

### show wireless radio

`{detail} {<DEVICE-NAME> {<1-3>|filter|on}}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
</tr>
<tr>
<td>radio</td>
<td>Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and Signal to Noise Ratio (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically. A radio’s RF Mode displays as:</td>
</tr>
<tr>
<td></td>
<td>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service</td>
</tr>
<tr>
<td></td>
<td>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service</td>
</tr>
<tr>
<td></td>
<td>• bridge – If it is configured to provide client-bridge operation</td>
</tr>
<tr>
<td>detail</td>
<td>Optional. Displays detailed radio operation status</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays detailed information for a specified radio. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.</td>
</tr>
<tr>
<td>&lt;1-3&gt;</td>
<td>Optional. Specify the radio interface index from 1 - 3 (if not specified as part of the radio ID)</td>
</tr>
<tr>
<td>filter &lt;RADIO-MAC&gt;</td>
<td>Optional. Provides additional filters</td>
</tr>
<tr>
<td></td>
<td>• &lt;RADIO-MAC&gt; – Optional. Filters based on the radio MAC address</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>
SHOW COMMANDS 6-163

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio</td>
<td>Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and Signal to Noise Ratio (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically. A radio’s RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation</td>
</tr>
<tr>
<td>detail</td>
<td>Optional. Displays detailed radio operation status</td>
</tr>
<tr>
<td>filter &lt;RADIO-MAC&gt;</td>
<td>Optional. Provides additional filter options • &lt;RADIO-MAC&gt; – Uses MAC address to filter radios</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is recursive and common to the ‘filter &lt;RADIO-MAC&gt;’ parameter: • on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain. • &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

- show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>} |
- rf {on <DEVICE-OR-DOMAIN-NAME>} |

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio</td>
<td>Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically. A radio’s RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation</td>
</tr>
<tr>
<td>statistics</td>
<td>Optional. Displays radio traffic and RF statistics</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Displays traffic and RF related statistics on a specified device or RF Domain • &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
<tr>
<td>rf {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>Optional. Displays RF statistics on a specified device or RF Domain • &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

- show wireless radio {statistics} {detail|window-data} {<DEVICE-NAME>} {<1-3>} |
- filter <RADIO-MAC>} {on <DEVICE-OR-DOMAIN-NAME>} |

<p>| wireless | Displays wireless configuration parameters |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `show wireless radio` | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and Signal to Noise Ratio (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically. A radio's RF Mode displays as:  
  - 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service  
  - 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service  
  - bridge – If it is configured to provide client-bridge operation |
| `tspec`          | Optional. Displays TSPEC information on a radio.                                                                                                                                                         |
| `<DEVICE-NAME>`  | Optional. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.                                                          |
| `filter`         | Optional. Provides additional filters  
  - `<RADIO-MAC>` – Optional. Filters based on the radio MAC address                                                                                                                                       |
| `on`             | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain.  
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.                                                                                  |
### SHOW COMMANDS 6-165

- **show wireless regulatory** [channel-info <WORD>|country-code <WORD>]

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>regulatory</td>
<td>Displays wireless regulatory information</td>
</tr>
<tr>
<td>channel-info &lt;WORD&gt;</td>
<td>Displays channel information</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the channel number.</td>
</tr>
<tr>
<td>country-code &lt;WORD&gt;</td>
<td>Displays country code to country name information</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the two letter ISO-3166 country code.</td>
</tr>
</tbody>
</table>

- **show wireless regulatory device-type** [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap7131|ap7161|ap7181|ap7502|ap7522|ap7532|ap7562|ap8132|ap8163|ap82xx|rfs4000] <WORD>

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>regulatory</td>
<td>Displays wireless regulatory information</td>
</tr>
<tr>
<td>device-type &lt;WORD&gt;</td>
<td>Displays wireless regulatory information based on the device type selected. Select the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP7131, AP7161, AP7181, AP7502, AP7522, AP7532, AP7562, AP8132, AP8163, AP82XX, RFS4000 (since RFS4011 is the only controller with radio, this option is used only to view RFS4011 wireless regulatory details).</td>
</tr>
<tr>
<td></td>
<td>After specifying the device type, specify the country code.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the two letter ISO-3166 country code.</td>
</tr>
</tbody>
</table>

- **show wireless rf-domain statistics** {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>rf-domain statistics</td>
<td>Displays RF Domain statistics</td>
</tr>
<tr>
<td>details</td>
<td>Optional. Displays detailed RF Domain statistics</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is recursive and common to the 'detail' parameter:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays RF Domain statistics on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

- **show wireless sensor-server** {on <DEVICE-OR-DOMAIN-NAME>}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor-server {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>Displays AirDefense sensor server configuration details</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays AirDefense sensor server configuration on a specified device or RF Domain</td>
</tr>
</tbody>
</table>

- **show wireless unsanctioned aps** {detailed|statistics} {<on <DEVICE-OR-DOMAIN-NAME>}}

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>unsanctioned aps</td>
<td>Displays unauthorized APs. Use additional filters to view specific details.</td>
</tr>
<tr>
<td>detailed</td>
<td>Optional. Displays detailed unauthorized APs information</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>**show wireless wips [client-blacklist</td>
<td>event-history] {on &lt;DEVICE-OR-DOMAIN-NAME&gt;**</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-OR-DOMAIN-NAME</strong></td>
<td>Displays the WIPS details</td>
</tr>
<tr>
<td>• client-blacklist – Displays blacklisted clients</td>
<td></td>
</tr>
<tr>
<td>• event-history – Displays event history</td>
<td></td>
</tr>
<tr>
<td>The following keyword is common to the 'client-blacklist' and 'event-history' parameters:</td>
<td></td>
</tr>
<tr>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays the WIPS details on a specified device or RF Domain.</td>
<td></td>
</tr>
<tr>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
<td></td>
</tr>
<tr>
<td>• show wlan [detail &lt;WLAN&gt;</td>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
</tr>
<tr>
<td><strong>wlan</strong></td>
<td>Displays WLAN related information based on the parameters passed</td>
</tr>
<tr>
<td><strong>detail &lt;WLAN&gt;</strong></td>
<td>Optional. Displays WLAN configuration</td>
</tr>
<tr>
<td>• &lt;WLAN&gt; – Specify the WLAN name.</td>
<td></td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</strong></td>
<td>Optional. Displays WLAN configuration on a specified device or RF Domain</td>
</tr>
<tr>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
<td></td>
</tr>
<tr>
<td><strong>policy-mappings</strong></td>
<td>Optional. Displays WLAN policy mappings</td>
</tr>
<tr>
<td><strong>usage-mappings</strong></td>
<td>Optional. Lists all devices and profiles using the WLAN</td>
</tr>
<tr>
<td>• show wlan {config filter [device &lt;DEVICE-NAME&gt;</td>
<td>rf-domain &lt;DOMAIN-NAME&gt;]}</td>
</tr>
<tr>
<td><strong>wlan</strong></td>
<td>Displays WLAN related information based on the parameters passed</td>
</tr>
<tr>
<td><strong>config filter</strong></td>
<td>Optional. Filters WLAN information based on the device name or RF Domain</td>
</tr>
<tr>
<td><strong>device &lt;DEVICE-NAME&gt;</strong></td>
<td>Optional. Filters WLAN information based on the device name</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the device name.</td>
<td></td>
</tr>
<tr>
<td><strong>rf-domain &lt;DOMAIN-NAME&gt;</strong></td>
<td>Optional. Filters WLAN information based on the RF Domain</td>
</tr>
<tr>
<td>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</td>
<td></td>
</tr>
<tr>
<td>• show wlan {statistics [&lt;WLAN&gt;</td>
<td>detail} {(on &lt;DEVICE-OR-DOMAIN-NAME&gt;)}</td>
</tr>
<tr>
<td><strong>wlan</strong></td>
<td>Displays WLAN related information based on the parameters passed</td>
</tr>
</tbody>
</table>
SHOW COMMANDS 6-167

Usage Guidelines

The customize command enables you to customize the `show > wireless` command output.

```
rfs7000-37FABE(config)#customize ?
hostname-column-width                  Customize hostname column width
show-adoption-status                   Customize the output of (show adoption status) command
show-wireless-client                  Customize the output of (show wireless client) command
show-wireless-client-stats           Customize the output of (show wireless client stats) command
show-wireless-client-stats-rf        Customize the output of (show wireless client stats rf) command
show-wireless-legacy-mesh-client-stats Customize the output of (show wireless legacy-mesh client stats) command
show-wireless-legacy-mesh-client-stats-detail Customize the output of (show wireless legacy-mesh client stats detail) command
show-wireless-legacy-mesh-client-stats-rf Customize the output of (show wireless legacy-mesh client stats rf) command
show-wireless-meshpoint              Customize the output of (show wireless meshpoint) command
show-wireless-meshpoint-accelerated-multicast Customize the output of (show wireless meshpoint accelerated-multicast) command
show-wireless-meshpoint-neighbor-stats Customize the output of (show wireless meshpoint neighbor stats) command
show-wireless-meshpoint-neighbor-stats-rf Customize the output of (show wireless meshpoint neighbor stats rf) command
show-wireless-radio                  Customize the output of (show wireless radio) command
show-wireless-radio-stats           Customize the output of (show wireless radio stats) command
show-wireless-radio-stats-rf        Customize the output of (show wireless radio stats rf) command
```

The default setting for the `show > wireless > client` command is as follows:

```
rfs7000-37FABE(config)#show wireless client
---------------------------------------------------------------------------------------
MAC      IPv4    VENDOR             RADIO-ID             WLAN                 VLAN         STATE
---------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------
Total number of wireless clients displayed: 0
```

The above output can be customized, using the `customize > show-wireless-client` command, as follows:
For more information on the customize command, see *customize*.

**Examples**

nx9500-6C8809(config)#show wireless wlan config

<table>
<thead>
<tr>
<th>NAME</th>
<th>ENABLE</th>
<th>SSID</th>
<th>ENCRYPTION</th>
<th>AUTHENTICATION</th>
<th>VLAN</th>
<th>BRIDGING MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>Y</td>
<td>test</td>
<td>wep64</td>
<td>none</td>
<td>1</td>
<td>local</td>
</tr>
</tbody>
</table>

 nx9500-6C8809(config)#

 nx9500-6C8809(config)#show wireless wips client-blacklist

No wireless clients blacklisted

 nx9500-6C8809(config)#

 nx9500-6C8809(config)#show wireless regulatory channel-info 1

Center frequency for channel 1 is 2412MHz

 nx9500-6C8809(config)#

 nx9500-6C8809(config)#show wireless regulatory country-code

<table>
<thead>
<tr>
<th>ISO CODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>gt</td>
<td>Guatemala</td>
</tr>
<tr>
<td>co</td>
<td>Colombia</td>
</tr>
<tr>
<td>cn</td>
<td>China</td>
</tr>
<tr>
<td>cm</td>
<td>Cameroon</td>
</tr>
<tr>
<td>cl</td>
<td>Chile</td>
</tr>
<tr>
<td>al</td>
<td>Albania</td>
</tr>
<tr>
<td>ca</td>
<td>Canada</td>
</tr>
<tr>
<td>gy</td>
<td>Guyana</td>
</tr>
<tr>
<td>hu</td>
<td>Hungary</td>
</tr>
</tbody>
</table>

--More--

 nx9500-6C8809(config)#

 nx9500-6C8809(config)#show wireless regulatory device-type ap650 us

<table>
<thead>
<tr>
<th>#</th>
<th>Channel Set</th>
<th>Power (mW)</th>
<th>Power (dBm)</th>
<th>Placement</th>
<th>DFS</th>
<th>CAC (mins)</th>
<th>TPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1-11</td>
<td>4000</td>
<td>36</td>
<td>Indoor/Outdoor</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>36-48</td>
<td>200</td>
<td>23</td>
<td>Indoor/Outdoor</td>
<td>Not Required</td>
<td>0</td>
<td>Not Required</td>
</tr>
<tr>
<td>3</td>
<td>52-64</td>
<td>500</td>
<td>27</td>
<td>Indoor/Outdoor</td>
<td>Required</td>
<td>1</td>
<td>Not Required</td>
</tr>
<tr>
<td>4</td>
<td>100-116</td>
<td>1000</td>
<td>30</td>
<td>Indoor/Outdoor</td>
<td>Not Required</td>
<td>1</td>
<td>Required</td>
</tr>
<tr>
<td>5</td>
<td>100-116</td>
<td>500</td>
<td>27</td>
<td>Indoor/Outdoor</td>
<td>Required</td>
<td>1</td>
<td>Not Required</td>
</tr>
<tr>
<td>6</td>
<td>100-116</td>
<td>1000</td>
<td>30</td>
<td>Indoor/Outdoor</td>
<td>Required</td>
<td>1</td>
<td>Required</td>
</tr>
<tr>
<td>7</td>
<td>132-140</td>
<td>500</td>
<td>27</td>
<td>Indoor/Outdoor</td>
<td>Required</td>
<td>1</td>
<td>Not Required</td>
</tr>
<tr>
<td>8</td>
<td>132-140</td>
<td>1000</td>
<td>30</td>
<td>Indoor/Outdoor</td>
<td>Required</td>
<td>1</td>
<td>Required</td>
</tr>
<tr>
<td>9</td>
<td>149-165</td>
<td>4000</td>
<td>36</td>
<td>Indoor/Outdoor</td>
<td>Not Required</td>
<td>0</td>
<td>Not Required</td>
</tr>
</tbody>
</table>

 nx9500-6C8809(config)#
rfs7000-37FABE(config)#show wireless ap detail

AP: B4-C7-99-71-17-28
   AP Name : ap8132-711728
   Location : default
   RF-Domain : default
   Type : ap81xx
   Model : AP-8132-66040-US
   IP : 10.2.0.99
   IPv6 : ::
   Num of radios : 2
   Num of clients : 0
   Last Smart-RF time : not done
   Stats update mode : auto
   Stats interval : 31
   Radio Modes :
      radio-1 : wlan
      radio-2 : wlan
   Country-code : us
   Site-Survivable : True
   Last error :
   Fault Detected : False

Power management information for ap81xx:
   Power management Mode : Auto
   Power management status : 3af
   Ethernet power status : all up
   Radio power status : all up

Total number of APs displayed: 1
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless ap load-balancing on rfs6000-81742D

Column Name Reference:
   Ap-Ld : Load of the AP as reported by it.
   Avg-Ld : Average AP load in the AP's neighborhood.
   2.4g-Ld : 2.4GHz band load in the AP's neighborhood.
   5g-Ld : 5GHz band load in the AP's neighborhood.
   Ap-2.4g-Ch-Ld : Load in the AP's 2.4GHz channel in its neighborhood.
   Avg-2.4g-Ch-Ld : Average load of a 2.4GHz channel in AP's neighborhood.
   Ap-5g-Ch-Ld : Load in the AP's 5GHz channel in its neighborhood.
   Avg-5g-Ch-Ld : Average load of a 5GHz channel in AP's neighborhood.
   Allow-2.4g-Req : AP responds to client requests on 2.4ghz radio
   Allow-5g-Req : AP responds to client requests on 5ghz radio

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rfs6000-81742D</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0:0</td>
<td>0:1</td>
<td>189%</td>
<td>196%</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0%</td>
<td>69%</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#
rfs7000-37FABE(config)#show wireless ap on default

----------------------------------------
| MODE | radio modes - W = WLAN, S=Sensor, ' ' (Space) = radio not present |
----------------------------------------
| AP-NAME | AP-LOCATION | RF-DOMAIN | AP-MAC | #RADIOS | MODE |
| #CLIENT | IPv4 | IPv6 |
----------------------------------------
| ap8132-711728 | default | B4-C7-99-71-17-28 | 2 | W-W | 0 |
10.2.0.99 | :: |
----------------------------------------

Total number of APs displayed: 1

nx6500-31FABE(config)#

rfs4000-1B3596#show wireless meshpoint tree

1: c00466 [5 MPs(3 roots, 2 bound)]
  - ap7131-96FAAC
    | - ap7131-96F998
    | - ap7131-96F6B4
   - ap622-7C0958
   - ap650-33DF84

2: test [3 MPs(0 roots, 0 bound)]
  *- ap7131-96F998
  *- ap7131-96FAAC
  *- ap7131-96F6B4

Total number of meshes displayed: 2

rfs4000-1B3596#

rfs4000-1B3596#show wireless meshpoint

----------------------------------------
<table>
<thead>
<tr>
<th>MESH</th>
<th>HOSTNAME</th>
<th>HOPS</th>
<th>IS-ROOT</th>
<th>CONFIG-AS-ROOT</th>
<th>ROOT-HOSTNAME</th>
<th>ROOT-BOUND-TIME</th>
<th>NEXT-HOP-HOSTNAME</th>
<th>NEXT-HOP-USE-TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>c00466</td>
<td>ap7131-96F998</td>
<td>1 NO</td>
<td>NO</td>
<td>ap7131-96FAAC</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
days 02:01:33 | ap7131-96FAC | 1 days 02:01:33 | c00466 | ap7131-96F998 | 0 YES | YES | N/A |
A N/A | N/A | c00466 | ap7131-96F6B4 | 2 NO | NO | ap7131-96FAAC | 1 |
days 02:01:31 | ap7131-96F998 | 1 days 02:01:31 | Total number of meshpoint displayed: 3 |
| rfs4000-1B3596# |

ap6532-000001#show wireless meshpoint multicast detail
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

----------------------------------------
<table>
<thead>
<tr>
<th>Group-Addr</th>
<th>Subscriber Name</th>
<th>Subscriber MPID</th>
<th>Timeout (mSecs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-00-5E-01-01-01</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
ap6532-000001#
**SHOW COMMANDS 6-171**

```
ap6532-000001#show wireless meshpoint neighbor detail
Neighbors @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Neighbor Name</th>
<th>Neighbor MPID.IFID</th>
<th>Root Name</th>
<th>Root MPID</th>
<th>RMem Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Interface</td>
<td>Auth-State</td>
<td>Resourced</td>
<td>Rank</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>97</td>
<td>87</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Init</td>
<td>Yes</td>
<td>0</td>
<td>97</td>
<td>86</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R1 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>93</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R1 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>94</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>87</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint proxy detail
Proxies @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Destination Addr</th>
<th>Owner Name</th>
<th>Owner MPID</th>
<th>Persist</th>
<th>VLAN</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-00-00-01</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>Permanent</td>
<td>101</td>
<td>180654310</td>
</tr>
<tr>
<td>00-1E-E5-A6-66-E2</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>Untimed</td>
<td>103</td>
<td>231920</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint multicast mesh1
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Group-Addr</th>
<th>Subscriber Name</th>
<th>Subscriber MPID</th>
<th>Timeout (mSecs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-00-5E-01-01-01</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>-1</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint path detail
Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Destination Name</th>
<th>Destination Addr</th>
<th>Next Hop Name</th>
<th>Next Hop IFID</th>
<th>State Hops</th>
<th>Type</th>
<th>Binding</th>
<th>Metric</th>
<th>Timeout</th>
<th>Path-Timeout</th>
<th>Sequence</th>
<th>MiNT ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-2E-AB-50</td>
<td>00-23-68-2E-AB-50 Valid 1</td>
<td>Root Bound</td>
<td>89</td>
<td>8730</td>
<td>0</td>
<td>23847</td>
<td>68.31.19.58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00-23-68-2E-97-60</td>
<td>00-23-68-2E-97-60 Valid 1</td>
<td>Root Unbound</td>
<td>92</td>
<td>5200</td>
<td>0</td>
<td>3481</td>
<td>68.31.1A.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint neighbor detail
Neighbors @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Neighbor Name</th>
<th>Neighbor MPID.IFID</th>
<th>Root Name</th>
<th>Root MPID</th>
<th>RMem Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Interface</td>
<td>Auth-State</td>
<td>Resourced</td>
<td>Rank</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>97</td>
<td>87</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Init</td>
<td>Yes</td>
<td>0</td>
<td>97</td>
<td>86</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R1 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>93</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R1 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>94</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>87</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint proxy detail
Proxies @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Destination Addr</th>
<th>Owner Name</th>
<th>Owner MPID</th>
<th>Persist</th>
<th>VLAN</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-00-00-01</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>Permanent</td>
<td>101</td>
<td>180654310</td>
</tr>
<tr>
<td>00-1E-E5-A6-66-E2</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>Untimed</td>
<td>103</td>
<td>231920</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint multicast mesh1
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Group-Addr</th>
<th>Subscriber Name</th>
<th>Subscriber MPID</th>
<th>Timeout (mSecs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-00-5E-01-01-01</td>
<td>ap6532-000001</td>
<td>00-23-68-2E-64-B2</td>
<td>-1</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint path detail
Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Destination Name</th>
<th>Destination Addr</th>
<th>Next Hop Name</th>
<th>Next Hop IFID</th>
<th>State Hops</th>
<th>Type</th>
<th>Binding</th>
<th>Metric</th>
<th>Timeout</th>
<th>Path-Timeout</th>
<th>Sequence</th>
<th>MiNT ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-2E-AB-50</td>
<td>00-23-68-2E-AB-50 Valid 1</td>
<td>Root Bound</td>
<td>89</td>
<td>8730</td>
<td>0</td>
<td>23847</td>
<td>68.31.19.58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00-23-68-2E-97-60</td>
<td>00-23-68-2E-97-60 Valid 1</td>
<td>Root Unbound</td>
<td>92</td>
<td>5200</td>
<td>0</td>
<td>3481</td>
<td>68.31.1A.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```

```
ap6532-000001#show wireless meshpoint neighbor detail
Neighbors @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

<table>
<thead>
<tr>
<th>Neighbor Name</th>
<th>Neighbor MPID.IFID</th>
<th>Root Name</th>
<th>Root MPID</th>
<th>RMem Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Interface</td>
<td>Auth-State</td>
<td>Resourced</td>
<td>Rank</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>97</td>
<td>87</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Init</td>
<td>Yes</td>
<td>0</td>
<td>97</td>
<td>86</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R1 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>93</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R1 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>94</td>
</tr>
<tr>
<td>Fixed 00-23-68-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>0</td>
<td>96</td>
<td>87</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1
```
rfs4000-22A24E#show wireless client

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VENDOR</th>
<th>RADIO-ID</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>STATE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Report start on RF-Domain: qs1

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VENDOR</th>
<th>RADIO-ID</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>STATE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Report end on RF-Domain: qs1

Report start on RF-Domain: Store-1

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VENDOR</th>
<th>RADIO-ID</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>STATE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Report end on RF-Domain: Store-1

Report start on RF-Domain: default

database not available

Report end on RF-Domain: default

Total number of clients displayed: 2

rfs4000-22A24E#

The following examples show client-bridge related information:

NX9500(config)#show adoption status

<table>
<thead>
<tr>
<th>DEVICE-NAME</th>
<th>VERSION</th>
<th>CFG-STAT</th>
<th>MSGS</th>
<th>ADOPTED-BY</th>
<th>LAST-ADOPTION</th>
<th>UPTIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap6562-167598</td>
<td>5.8.1.0-046R configured</td>
<td>No</td>
<td>NX9500</td>
<td>0 days 00:01:59</td>
<td>0 days 00:03:22</td>
<td></td>
</tr>
</tbody>
</table>

Total number of devices displayed: 1

NX9500(config)#

NX9500(config)#show wireless bridge on ap6562-167598

<table>
<thead>
<tr>
<th>LOCAL RADIO ACTIVITY (sec ago)</th>
<th>LOCAL BSSID</th>
<th>SELECTED AP</th>
<th>RF-BAND</th>
<th>CHANNEL</th>
<th>STATE</th>
<th>UP TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap6562-167598:R2 FC-0A-81-16-69-50 B4-C7-99-CA-A1-F0 5GHz</td>
<td>00:00:00:00</td>
<td>104</td>
<td>Selected</td>
<td>0 days 00:01:55</td>
<td>00:00:00</td>
<td></td>
</tr>
</tbody>
</table>

Total number of radios displayed: 1

NX9500(config)#
NX9500(config)# show wireless bridge config

<table>
<thead>
<tr>
<th>IDX</th>
<th>NAME</th>
<th>MAC</th>
<th>PROFILE</th>
<th>RF-DOMAIN</th>
<th>SSID</th>
<th>BAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap6562-167598</td>
<td>FC-0A-81-16-75-98</td>
<td>default-ap6562</td>
<td>default</td>
<td>inf_ap</td>
<td>2.4GHz/5GHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ccmp</td>
<td>eap</td>
<td>hoabeo</td>
<td></td>
</tr>
</tbody>
</table>

NX9500(config)# show wireless bridge hosts

<table>
<thead>
<tr>
<th>HOST MAC</th>
<th>BRIDGE MAC</th>
<th>IP</th>
<th>BRIDGING STATUS</th>
<th>ACTIVITY (sec ago)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-0A-81-16-75-98</td>
<td>FC-0A-81-16-69-50</td>
<td>172.16.34.55</td>
<td>UP</td>
<td>00:00:00</td>
</tr>
</tbody>
</table>

Total number of hosts displayed: 1

NX9500(config)# show wireless bridge statistics

<table>
<thead>
<tr>
<th>LOCAL RADIO</th>
<th>CONNECTED AP</th>
<th>SIGNAL (dbm)</th>
<th>SNR</th>
<th>TX-RATE (Mbps)</th>
<th>RX-RATE (Mbps)</th>
<th>Tx bps</th>
<th>Rx bps</th>
<th>RETRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap6562-167598:R2</td>
<td>B4-C7-99-CA-A1-F0</td>
<td>-52</td>
<td>50</td>
<td>53</td>
<td>36</td>
<td>1 k</td>
<td>3 k</td>
<td>10</td>
</tr>
</tbody>
</table>

Total number of radios displayed: 1

NX9500(config)# show wireless bridge candidate-ap on ap6562-167598

Client Bridge Candidate APs:

<table>
<thead>
<tr>
<th>AP-MAC</th>
<th>BAND</th>
<th>CHANNEL</th>
<th>SIGNAL (dbm)</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>B4-C7-99-CA-A1-F0</td>
<td>5 GHz</td>
<td>104</td>
<td>-39</td>
<td>selected</td>
</tr>
</tbody>
</table>

Total number of candidates displayed: 1

NX9500(config)# show wireless bridge certificate status on ap6562-167598

Certificate Last Updated Status: Thu Jul 23 11:41:40 2015

NX9500(config)#
### 6.1.74 wwan

**show commands**

Displays wireless WAN status

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- `show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wwan</td>
<td>Displays wireless WAN configuration and status details</td>
</tr>
<tr>
<td>configuration</td>
<td>Displays wireless WAN configuration information</td>
</tr>
<tr>
<td>status</td>
<td>Displays wireless WAN status information</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is common to the 'configuration' and 'status' parameters:</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays configuration or status details on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan configuration
>>> WWAN Configuration:
+-------------------------------------------
| Access Port Name : isp.cingular           |
| User Name        : testuser                |
| Cryptomap        : map1                    |
+-------------------------------------------
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan status
>>> WWAN Status:
+-------------------------------------------
| State : ACTIVE                            |
| DNS1  : 209.183.54.151                    |
| DNS2  : 209.183.54.151                    |
+-------------------------------------------
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs7000-37FABE(config)#show wwan configuration
>>> WWAN Configuration:
+-------------------------------------------
| Access Port Name : None                    |
| User Name        : None                    |
+-------------------------------------------
rfs7000-37FABE(config)#
```
### 6.1.75 slot

> **show commands**

Displays *Peripheral Component Interconnect* (PCI) express slot statistics. Use this command to view if the slots have been used for Team-Centro VM or WING support.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

`show slot`

**Parameters**
- `slot` slot

<table>
<thead>
<tr>
<th>slot</th>
<th>Shows PCI express card statistics</th>
</tr>
</thead>
</table>

**Examples**

```
nx4500-5CFA2B>show slot
-----------------------------
SLOT TYPE MODULE   STATUS
-----------------------------
1    []   wing   Enabled
2    []   wing   Enabled
3    []   wing   Enabled
4    []   wing   Enabled
-----------------------------
nx4500-5CFA2B>
```
6.1.76 smart-cache

show commands
Displays details on the cached entry for a specific URL or all URLs

NOTE: Smart content caching is a licensed feature and can be enabled only if a license is procured and applied to the device. For more information, see smart-rf-policy.

Supported in the following platforms:
• Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

Syntax
show smart-cache [active-requests|clients|purge-requests|statistics content-type|storage] {on <DEVICE-NAME>}

Parameters
• show smart-cache [active-requests|clients|purge-requests|statistics content-type|storage] {on <DEVICE-NAME>}

Examples
nx4500-5CFA2B>show smart-cache statistics
Warning: no smart-cache license installed, smart-cache is not running.
Warning: name-server not configured, smart-cache may not work.
-------------------------------------------------------------------------------
| DURATION   | DATA (KB)   | BANDWIDTH (Kbps) | REQUESTS |
|            | TOTAL CACHE | WAN CACHE        | TOTAL CACHE |
| Since boot | 0           | 0.0              | 0          |
-------------------------------------------------------------------------------

nx4500-5CFA2B(config)#show smart-cache statistics content-type

<table>
<thead>
<tr>
<th>DURATION</th>
<th>VIDEO (KB)</th>
<th>AUDIO (KB)</th>
<th>IMAGE (KB)</th>
<th>TEXT (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TOTAL CACHE</td>
<td>TOTAL CACHE</td>
<td>TOTAL CACHE</td>
<td>TOTAL CACHE</td>
</tr>
<tr>
<td>Since boot</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B(config)#
```
show smart-cache storage

<table>
<thead>
<tr>
<th>USED</th>
<th>TOTAL</th>
<th>USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 MB</td>
<td>DISABLED</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B#`
```
6.1.77 virtual-machine

show commands

Displays the virtual-machine (VM) configuration, logs, and statistics

Supported in the following platforms:
  • Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

show virtual-machine [configuration|debugging|export|statistics]

show virtual-machine [configuration|statistics] {<VM-NAME>|team-urc|team-rls|team-vowlan} {(on <DEVICE-NAME>)}

show virtual-machine debugging {level|on}
show virtual-machine debugging {level [debug|error|info|warning]} {on <DEVICE-NAME>}

show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}

The NX9500 and NX9510 series service platforms support ADSP and TEAM-CMT virtual machines only. The following show commands are specific to the NX9500 and NX9510 devices:

show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt}

Parameters

• show virtual-machine [configuration|statistics] {<VM-NAME>|team-urc|team-rls|team-vowlan} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>virtual-machine</th>
<th>Displays the following VM-related information: configuration or statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Displays detailed VM configuration</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays VM statistics</td>
</tr>
<tr>
<td>[ &lt;VM-NAME&gt;</td>
<td>team-urc</td>
</tr>
<tr>
<td></td>
<td>• &lt;VM-NAME&gt; – Optional. Displays VM configuration or statistics for the virtual machine identified by the &lt;VM-NAME&gt; keyword. Specify the VM name.</td>
</tr>
<tr>
<td></td>
<td>• team-urc – Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics</td>
</tr>
<tr>
<td></td>
<td>• team-rls – Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/statistics</td>
</tr>
<tr>
<td></td>
<td>• team-vowlan – Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics</td>
</tr>
<tr>
<td></td>
<td>Note: These keywords are specific to the NX45XX and NX65XX series service platforms.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Specifies the name of the device on which the command is executed</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the service platform.</td>
</tr>
</tbody>
</table>

• show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt} {(on <DEVICE-NAME>)}

<table>
<thead>
<tr>
<th>virtual-machine</th>
<th>Displays the following VM-related information: configuration or statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Displays detailed VM configuration</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays VM statistics</td>
</tr>
</tbody>
</table>
### Command Syntax

```
show virtual-machine configuration team-urc
VM: team-urc
  autostart       : start
  bootloader      : /usr/bin/pygrub
  cpus            : ['3', '2']
  disk            : file:/vms/test/team-centro/disk,xvda,w
  maxmem          : 3584 MB
  maxvcpus        : 2
  memory          : 1200 MB
  name            : team-urc
  on_crash        : coredump-restart
  on_poweroff     : destroy
  on_reboot       : restart
  serial          : pty
  tty             : /dev/pts/1
  uuid            : b80f8e19-a1f6-02c9-cbbc-10c1ae0a170
```

### Command Description

- **Show Commands**: Displays the following VM-related information: configuration or statistics.
- **Virtual Machine**: Displays VM logs.
- **Export**: Displays VM configuration export related information.
- **Level**: Optional. Displays VM logs based on the selected level.
- **Device Name**: Optional. Specifies the name of the device on which the command is executed.

### Examples

```
nx4500-5CFA2B# show virtual-machine configuration team-urc
VM: team-urc
  autostart       : start
  bootloader      : /usr/bin/pygrub
  cpus            : ['3', '2']
  disk            : file:/vms/test/team-centro/disk,xvda,w
  maxmem          : 3584 MB
  maxvcpus        : 2
  memory          : 1200 MB
  name            : team-urc
  on_crash        : coredump-restart
  on_poweroff     : destroy
  on_reboot       : restart
  serial          : pty
  tty             : /dev/pts/1
  uuid            : b80f8e19-a1f6-02c9-cbbc-10c1ae0a170
```
vcpus : 1
vif : bridge=vm2br, mac=B4:C7:99:5C:FA:2F, script=vif-bridge, type=bridge
     : bridge=brpriv, mac=00:16:3e:65:ff:01, script=vif-bridge
     : bridge=vm3br, mac=B4:C7:99:5C:FA:31, script=vif-bridge, type=bridge

nx4500-5CFA2B#

nx4500-5CFA2B# show virtual-machine configuration

<table>
<thead>
<tr>
<th>NAME</th>
<th>AUTOSTART</th>
<th>MEMORY (MB)</th>
<th>VCPUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>team-rls</td>
<td>start</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>team-urc</td>
<td>start</td>
<td>1200</td>
<td>1</td>
</tr>
<tr>
<td>team-vowlan</td>
<td>start</td>
<td>1500</td>
<td>1</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B#

nx4500-5CFA2B# show virtual-machine statistics

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATE</th>
<th>VCPUS</th>
<th>MEM (MB)</th>
<th>BRIDGE-IF</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiNG</td>
<td>-</td>
<td>-</td>
<td>1009</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>team-rls</td>
<td>(not_installed)</td>
<td>-</td>
<td>1200</td>
<td>eth0 (vmif2)</td>
<td>192.168.13.103</td>
</tr>
<tr>
<td>team-urc</td>
<td>Running</td>
<td>1</td>
<td>1200</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>team-vowlan</td>
<td>(not_installed)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B#

The following example shows WiNG memory allocation on a NX9500 device:

nx9500-6C874D# show virtual-machine statistics

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATE</th>
<th>VCPUS</th>
<th>MEM (MB)</th>
<th>BRIDGE-IF</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiNG</td>
<td>-</td>
<td>-</td>
<td>18432</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>adsp</td>
<td>Halted</td>
<td>-</td>
<td>-</td>
<td>unknown</td>
<td>-</td>
</tr>
<tr>
<td>team-cmt</td>
<td>Halted</td>
<td>-</td>
<td>unknown</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

nx9500-6C874D#

nx9500-6C874D# show virtual-machine configuration

<table>
<thead>
<tr>
<th>NAME</th>
<th>AUTOSTART</th>
<th>MEMORY (MB)</th>
<th>VCPUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiNG</td>
<td>-</td>
<td>18432</td>
<td>-</td>
</tr>
<tr>
<td>adsp</td>
<td>ignore</td>
<td>12000</td>
<td>12</td>
</tr>
<tr>
<td>team-cmt</td>
<td>ignore</td>
<td>1024</td>
<td>1</td>
</tr>
</tbody>
</table>

nx9500-6C874D#

nx9500-6C874D> show virtual-machine statistics adsp
VM name: adsp
Base Version : unknown
Install Status : not_installed

nx9500-6C874D>
6.1.78 mirroring

*show commands*

Displays the port mirroring sessions

For more information on configuring port mirroring sessions, see *mirror*.

Supported in the following platforms:

- Service Platforms — NX4524, NX6524

**Syntax**

`show mirroring`

**Parameters**

- `show mirroring`

<table>
<thead>
<tr>
<th>mirroring</th>
<th>Displays the port mirroring sessions</th>
</tr>
</thead>
</table>

**Examples**

```
nx4524-470984#show mirroring
+---------+----------+----------+--------+
| Session | Source   | Destination | Direction |
+---------+----------+----------+--------+
| 1       | ge3      | ge24     | any    |
| 2       | ge7      | ge24     | inbound|
| 3       | ge5      | ge24     | outbound|
+---------+----------+----------+--------+
nx4524-470984#    ```
6.1.79 raid

- show commands

Displays Redundant Array of Independent Disks (RAID) related information, such as array status, consistency check status, and RAID log.

Use this command to assess the RAID array’s drive utilization and whether the drives are currently online. Since there is only one RAID array controller reporting status to the service platform, it is important to know if other drives house hot spare drives as additional resources should one of the dedicated drives fail. This command also displays whether a physical within the RAID array has a drive installed, and whether the drive is currently online.

For more information on configuring RAID, see raid.

Supported in the following platforms:
- Service Platforms — NX9500

**Syntax**

show raid {on <DEVICE-NAME>}

**Parameters**

- show raid {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>raid on &lt;DEVICE-NAME&gt;</th>
<th>Displays the RAID array status and statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Displays RAID status and statistics on a specified device</td>
<td></td>
</tr>
<tr>
<td>- &lt;DEVICE-NAME&gt; — Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

nx9500-6C874D(config)#show raid
Logical drive info:
  Size 930 GB, State optimal
  Alarm enabled
  Last check: Sat Aug 10 02:56:54 2013
  Last check result: ending

Physical drive info:

  Drive  0: online
  Drive  1: online
  Drive  2: not-installed
  Drive  3: not-installed
  Drive  4: not-installed

nx9500-6C874D(config)#
Profiles enable administrators to assign a common set of configuration parameters, policies, WLANs, wireless parameters, and security parameters to service platforms, wireless controllers, and access points across a large, multi-segment site. The configuration parameters within a profile are based on the hardware model the profile was created to support.

The service platforms, wireless controllers, and access points support both default and user-defined profiles. Each default and user-defined profile contains policies and configurations that are applied to devices assigned to the profile. Changes made to these configurations are automatically inherited by the assigned devices. Therefore, the central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

Default profiles are system maintained and are automatically applied to service platforms and wireless controllers. The default AP profile is automatically applied to an AP (discovered by a wireless controller or service platform) unless an AP auto-provisioning policy is defined specifically assigning the AP to a user-defined profile. After adoption, changes made to a profile’s parameters are reflected across all devices using the profile. Default profiles are ideal for single site deployments where service platforms, wireless controllers, and access points share a common configuration.

User-defined profiles, on the other hand, are manually created for each supported service platform, wireless controller, and access point model. The use of user-defined profiles is recommended in larger deployments when groups of devices (on different floors, buildings, or sites) share a common configuration. These user-defined profiles can be manually or automatically assigned to access points using an AP auto-provisioning policy. An AP auto-provisioning policy provides the means to assign profiles to access points based on model, serial number, VLAN ID, DHCP options, IP address (subnet) and MAC address. For more information, see Chapter 9, AUTO-PROVISIONING-POLICY.

A user-defined profile can be created for each of the following device type:

- AP621 – Adds an AP621 access point profile
- AP622 – Adds an AP622 access point profile
- AP650 – Adds an AP650 access point profile
- AP6511 – Adds an AP6511 access point profile
- AP6521 – Adds an AP6521 access point profile
- AP6522 – Adds an AP6522 access point profile
- AP6532 – Adds an AP6532 access point profile
- AP6562 – Adds an AP6562 access point profile
- AP71XX – Adds an AP71XX access point profile supporting the AP7131, AP7161, and AP7181 models
- AP7502 – Adds an AP7502 access point profile
• AP7522 – Adds an AP7522 access point profile
• AP7532 – Adds an AP7532 access point profile
• AP7562 – Adds an AP7562 access point profile
• AP81XX – Adds an AP81XX access point profile supporting the AP8122, AP8132, and AP8163 models
• AP82XX – Adds an AP82XX access point profile supporting the AP8222 and AP8232 models
• EX3524 – Adds an EX3524 wireless controller profile
• EX3548 – Adds an EX3548 wireless controller profile
• RFS4000 – Adds an RFS4000 wireless controller profile
• RFS6000 – Adds an RFS6000 wireless controller profile
• RFS7000 – Adds an RFS7000 wireless controller profile
• NX45XX – Adds an NX45XX series service platform profile supporting the NX4500 and NX4524 models
• NX5500 – Adds an NX5500 wireless controller profile
• NX65XX – Adds an NX65XX series service platform profile supporting the NX6500 and NX6524 models
• NX7500 – Adds an NX75XX series service platform profile supporting the NX7510, NX7520, and NX7530 models
• NX9XXX – Adds an NX9XXX series service platform profile supporting the NX9000, NX9500, and NX9510 models
• NX9600 – Adds an NX9600 service platform profile. Supported only on a NX9600 model device.
• T5 – Adds a T5 controller profile
• vx9000 – Adds a VX9000 profile

NOTE: A T5 profile can be created only on the following platforms: RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, and NX9510.

NOTE: A VX9000 profile can be created only on the NX9000 series service platforms.

Although profiles assign a common set of configuration parameters across devices, individual devices can still be assigned unique configuration parameters that follow the flat configuration model. As individual device updates are made, these devices no longer share the profile based configuration they originally supported. Therefore, changes made to a profile are not automatically inherited by devices who have had their configuration customized. These devices require careful administration, as they cannot be tracked as profile members. Their customized configurations overwrite their profile configurations until the profile is re-applied.

NOTE: The commands present under ‘Profiles’ are also available under the ‘Device mode’. The additional commands specific to the ‘Device mode’ are listed separately.

This chapter is organized into the following topics:
• Profile Config Commands
• Device Config Commands
• T5 Profile Config Commands
• EX3524 & EX3548 Profile/Device Config Commands
To view the list of device profiles supported, use the following command:

```
<DEVICE>(config)#profile ?
anyap       Any access point profile
ap621       AP621 access point profile
ap622       AP622 access point profile
ap650       AP650 access point profile
ap6511      AP6511 access point profile
ap6521      AP6521 access point profile
ap6522      AP6522 access point profile
ap6532      AP6532 access point profile
ap6562      AP6562 access point profile
ap71xx      AP71XX access point profile
ap7502      AP7502 access point profile
ap7522      AP7522 access point profile
ap7532      AP7532 access point profile
ap7562      AP7562 access point profile
ap81xx      AP81XX access point profile
ap82xx      AP82XX access point profile
containing Specify profiles that contain a sub-string in the profile name
ex3524      EX3524 wireless controller profile
ex3548      EX3548 wireless controller profile
filter      Specify addition selection filter
nx45xx      NX45XX integrated services platform profile
nx5500      NX5500 wireless controller profile
nx65xx      NX65XX integrated services platform profile
nx75xx      NX75XX wireless controller profile
nx9000      NX9000 wireless controller profile
nx9600      NX9600 wireless controller profile
rfs4000      RFS4000 wireless controller profile
rfs6000      RFS6000 wireless controller profile
rfs7000      RFS7000 wireless controller profile
t5          T5 wireless controller profile
vx9000      VX9000 wireless controller profile
```

```
<DEVICE>(config)#
```

```
<rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#
```

```
<rfs7000-37FABE(config)#profile ap71xx default-ap71xx
rfs7000-37FABE(config-profile-default-ap71xx)#
```

The following example shows the commands specific to a NX45XX and NX65XX series service platform profile:

```
nx4500-5CFA2B(config)#profile ?
anyap       Any access point profile
ap621       AP621 access point profile
ap622       AP622 access point profile
ap650       AP650 access point profile
ap6511      AP6511 access point profile
ap6521      AP6521 access point profile
ap6522      AP6522 access point profile
ap6532      AP6532 access point profile
ap6562      AP6562 access point profile
ap71xx      AP71XX access point profile
ap7502      AP7502 access point profile
ap7522      AP7522 access point profile
ap7532      AP7532 access point profile
ap7562      AP7562 access point profile
ap81xx      AP81XX access point profile
ap82xx      AP82XX access point profile
containing Specify profiles that contain a sub-string in the profile name
ex3524      EX3524 wireless controller profile
ex3548      EX3548 wireless controller profile
filter      Specify addition selection filter
nx45xx      NX45XX integrated services platform profile
nx65xx      NX65XX integrated services platform profile
rfs4000      RFS4000 wireless controller profile
rfs6000      RFS6000 wireless controller profile
rfs7000      RFS7000 wireless controller profile
```

```
nx4500-5CFA2B(config)#
```
t5          T5 wireless controller profile
<cr>

nx4500-5CFA2B(config)#

<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#?

Profile Mode commands:
adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning policy when adopted by another controller
adoption                                   Adoption configuration
alias                                      Alias
application-policy                        Application Policy configuration
area                                       Set name of area where the system is located
arp                                        Address Resolution Protocol (ARP)
auto-learn-staging-config                 Enable learning network configuration of the devices that come for adoption
autogen-uniqueid                          Autogenerate a unique id
autoinstall                               Autoinstall settings
bluetooth-detection                       Detect Bluetooth devices using the Bluetooth USB module
bridge                                     Ethernet bridge
captive-portal                            Captive portal
cdp                                        Cisco Discovery Protocol
cluster                                    Cluster configuration
configuration-persistence                 Enable persistence of configuration across reloads (startup config file)
controller                                WLAN controller configuration
critical-resource                        Critical Resources
database-backup                           Scheduled Database Backup
crypto                                     Encryption related commands
device-upgrade                             Device firmware upgrade
dot1x                                      802.1X
dpi                                        Enable Deep-Packet-Inspection (Application Assurance)
dscp-mapping                              Configure IP DSCP to 802.1p priority mapping for untagged frames
e-mail-notification                       Email notification configuration
enforce-version                           Check the firmware versions of devices before interoperating
environmental-sensor                      Environmental Sensors Configuration
events                                     System event messages
export                                     Export a file
file-sync                                  File sync between controller and adoptees
floor                                      Set the floor within a area where the system is located
gre                                        GRE protocol
http-analyze                              Specify HTTP-Analysis configuration
interface                                 Select an interface to configure
ip                                         Internet Protocol (IP)
ipv6                                       Internet Protocol version 6 (IPv6)
l2tpv3                                     L2tpv3 protocol
l3e-lite-table                            L3e lite Table
led                                        Turn LEDs on/off on the device
led-timeout                                Configure the time for the led to turn off after the last radio state change
legacy-auto-downgrade                     Enable device firmware to auto downgrade when other legacy devices are detected
legacy-auto-update                        Auto upgrade of legacy devices
lldp                                       Link Layer Discovery Protocol
load-balancing Configure load balancing parameter
logging Modify message logging facilities
mac-address-table MAC Address Table
mac-auth 802.1X
memory-profile Memory profile to be used on the device
meshpoint-device Configure meshpoint device parameters
meshpoint-monitor-interval Configure meshpoint monitoring interval
min-misconfiguration-recovery-time Check controller connectivity after configuration is received
mint MiNT protocol
misconfiguration-recovery-time Configure neighbor inactivity timeout
neighbor-inactivity-timeout Configure neighbor information exchange interval
no Negate a command or set its defaults
noc Configure the noc related setting
ntp Ntp server A.B.C.D
offline-duration Set duration for which a device remains unadopted before it generates offline event
power-config Configure power mode
preferred-controller-group Controller group this system will prefer for adoption
preferred-tunnel-controller Tunnel Controller Name this system will prefer for tunneling extended vlan traffic
radius Configure device-level radius authentication parameters
raid RAID
remove-override Remove configuration item override from the device (so profile value takes effect)
rf-domain-manager RF Domain Manager
router Dynamic routing
slot PCI expansion Slot
spanning-tree Spanning tree
traffic-class-mapping Configure IPv6 traffic class to 802.1p priority mapping for untagged frames
traffic-shape Traffic shaping
trustpoint Assign a trustpoint to a service
tunnel-controller Tunnel Controller group this controller belongs to
use Set setting to use
vrrp VRRP configuration
vrrp-state-check Publish interface via OSPF/BGP only if the interface VRRP state is not BACKUP
wep-shared-key-auth Enable support for 802.11 WEP shared key authentication
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode[end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write

Write running configuration to memory or terminal

<DEVICE>(config-profile-<PROFILE-NAME>)#

<DEVICE>(config-profile-<T5-PROFILE-NAME>)#?

T5 Profile Mode commands:
cpe T5 CPE configuration
interface Select an interface to configure
ip Internet Protocol (IP)
no Negate a command or set its defaults
ntp Configure NTP
override-wlan Configure RF Domain level overrides for wlan
t5 T5 configuration
t5-logging Modify message logging facilities
use Set setting to use
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

<DEVICE>(config-profile-<T5-PROFILE-NAME>)#

<DEVICE>(config-profile-<EX3524/EX3548-PROFILE-NAME>)#?

EX3500 Profile Mode commands:
interface Select an interface to configure
ip Internet Protocol (IP)
no Negate a command or set its defaults
power Ex3500 Power over Ethernet Command
upgrade Configures upgrade option for ex3500 system
use Set setting to use
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

<DEVICE>(config-profile-<EX3524/EX3548-PROFILE-NAME>)#

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
# 7.1 Profile Config Commands

The following table summarizes profile configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopter-auto-provisioning-policy-lookup</td>
<td>Enables the use of a centralized auto provisioning policy on this profile</td>
<td>page 7-11</td>
</tr>
<tr>
<td>adoption</td>
<td>Configures a minimum and maximum delay time in the initiation of the device adoption process</td>
<td>page 7-12</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, network-group, network-service, VLAN, and string aliases on this profile</td>
<td>page 7-13</td>
</tr>
<tr>
<td>application-policy</td>
<td>Associates a RADIUS server provided application policy with this profile. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane.</td>
<td>page 7-20</td>
</tr>
<tr>
<td>area</td>
<td>Sets the system’s area of location (the area name)</td>
<td>page 7-21</td>
</tr>
<tr>
<td>arp</td>
<td>Configures static address resolution protocol</td>
<td>page 7-22</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enables network configuration learning of devices</td>
<td>page 7-24</td>
</tr>
<tr>
<td>autogen-uniqueid</td>
<td>Autogenerates a unique local ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device.</td>
<td>page 7-25</td>
</tr>
<tr>
<td>autoinstall</td>
<td>Configures the automatic install feature</td>
<td>page 7-27</td>
</tr>
<tr>
<td>bluetooth-detection</td>
<td>Enables detection of Bluetooth devices. These are devices using the Bluetooth USB module.</td>
<td>page 7-28</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures bridge specific parameters</td>
<td>page 7-29</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures captive portal advanced Web page upload on a device profile</td>
<td>page 7-55</td>
</tr>
<tr>
<td>cdp</td>
<td>Enables Cisco Discovery Protocol (CDP) on a device</td>
<td>page 7-56</td>
</tr>
<tr>
<td>cluster</td>
<td>Configures a cluster name</td>
<td>page 7-57</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enables persistence of configuration across reloads</td>
<td>page 7-60</td>
</tr>
<tr>
<td>controller</td>
<td>Configures a wireless controller or service platform</td>
<td>page 7-61</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Monitors resources that are critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses.</td>
<td>page 7-65</td>
</tr>
<tr>
<td>crypto</td>
<td>Configures data encryption related protocols and settings</td>
<td>page 7-72</td>
</tr>
<tr>
<td>database-backup</td>
<td>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server. When applied to devices, this profile enables the back up of the specified database.</td>
<td>page 7-133</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings on this profile</td>
<td>page 7-134</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures 802.1x standard authentication controls</td>
<td>page 7-136</td>
</tr>
<tr>
<td>dpi</td>
<td>Enables Deep Packet Inspection (DPI) on this profile</td>
<td>page 7-138</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configures an IP DSCP to 802.1p priority mapping for untagged frames</td>
<td>page 7-140</td>
</tr>
<tr>
<td>email-notification</td>
<td>Configures e-mail notification settings</td>
<td>page 7-141</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Enables checking of a device's firmware version before attempting adoption or clustering</td>
<td>page 7-143</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Configures the environmental sensor settings on this profile (applicable to AP8132 model access point only)</td>
<td>page 7-144</td>
</tr>
<tr>
<td>events</td>
<td>Enables system event logging and message generation. This command also configures event message forwarding settings.</td>
<td>page 7-146</td>
</tr>
<tr>
<td>export</td>
<td>Enables export of startup.log file after every boot</td>
<td>page 7-147</td>
</tr>
<tr>
<td>file-sync</td>
<td>Configures parameters enabling synching of PKCS#12 certificate between the staging-controller and adoptee AP6522/AP6562 client bridges</td>
<td>page 7-148</td>
</tr>
<tr>
<td>floor</td>
<td>Sets the floor name where the system is located</td>
<td>page 7-149</td>
</tr>
<tr>
<td>gre</td>
<td>Enables Generic Routing Encapsulation (GRE) tunneling on this profile</td>
<td>page 7-150</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Configures HTTP analysis settings</td>
<td>page 7-162</td>
</tr>
<tr>
<td>http-analyze (NX45XX, NX65XX, and NX9000)</td>
<td>Configures HTTP analysis settings on a NX series service platform</td>
<td>page 7-164</td>
</tr>
<tr>
<td>interface</td>
<td>Configures an interface (VLAN, radio, GE etc.)</td>
<td>page 7-167</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IPv4 components</td>
<td>page 7-347</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures IPv6 components</td>
<td>page 7-357</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Defines the Layer 2 Tunnel Protocol (L2TP) protocol for tunneling layer 2 payloads using Virtual Private Networks (VPNs)</td>
<td>page 7-361</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>Configures L3e Lite Table with this profile</td>
<td>page 7-363</td>
</tr>
<tr>
<td>led</td>
<td>Turns device LEDs on or off</td>
<td>page 7-364</td>
</tr>
<tr>
<td>led-timeout</td>
<td>Configures LED-timeout timer. This command is specific to the NX9000 series service platforms.</td>
<td>page 7-365</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Auto downgrades a legacy device firmware</td>
<td>page 7-367</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto upgrades a legacy device firmware</td>
<td>page 7-368</td>
</tr>
<tr>
<td>lldp</td>
<td>Configures Link Layer Discovery Protocol (LLDP)</td>
<td>page 7-369</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configures load balancing parameters</td>
<td>page 7-371</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging settings</td>
<td>page 7-376</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Configures the MAC address table</td>
<td>page 7-378</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables 802.1x user authentication protocol on this profile</td>
<td>page 7-380</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Configures the memory profile used on the device</td>
<td>page 7-383</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configures a meshpoint device parameters</td>
<td>page 7-384</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configures meshpoint monitoring interval</td>
<td>page 7-385</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Configures the minimum device connectivity verification time</td>
<td>page 7-386</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol settings</td>
<td>page 7-387</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Verifies device connectivity after a configuration is received</td>
<td>page 7-394</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configures neighbor inactivity timeout</td>
<td>page 7-395</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configures neighbor information exchange interval</td>
<td>page 7-396</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts settings to their default. The no command, when used in the profile configuration mode, removes the selected profile’s settings or reverts them to their default.</td>
<td>page 7-397</td>
</tr>
<tr>
<td>noc</td>
<td>Configures NOC settings</td>
<td>page 7-399</td>
</tr>
<tr>
<td>ntp</td>
<td>Configures NTP server settings</td>
<td>page 7-400</td>
</tr>
<tr>
<td>offline-duration</td>
<td>Sets the duration, in minutes, for which a device remains unadopted before it generates offline event</td>
<td>page 7-403</td>
</tr>
<tr>
<td>power-config</td>
<td>Configures the power mode</td>
<td>page 7-404</td>
</tr>
<tr>
<td>preferred-controller-group</td>
<td>Specifies the wireless controller or service platform group preferred for adoption</td>
<td>page 7-406</td>
</tr>
<tr>
<td>preferred-tunnel-controller</td>
<td>Configures the tunnel wireless controller or service platform preferred by the system to tunnel extended VLAN traffic</td>
<td>page 7-407</td>
</tr>
<tr>
<td>radius</td>
<td>Configures device-level RADIUS authentication parameters</td>
<td>page 7-408</td>
</tr>
<tr>
<td>raid</td>
<td>Enables alarm on the array. This command is supported only on the NX9500 and NX9510 series service platform profile/device config modes.</td>
<td>page 7-474</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Enables devices using this profile to be elected as RF Domain manager. Also sets the priority value for devices using this profile in the RF Domain manager election process.</td>
<td>page 7-409</td>
</tr>
<tr>
<td>router</td>
<td>Configures dynamic router protocol settings</td>
<td>page 7-410</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Configures spanning tree related settings</td>
<td>page 7-412</td>
</tr>
<tr>
<td>traffic-class-mapping</td>
<td>Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority</td>
<td>page 7-415</td>
</tr>
<tr>
<td>traffic-shape</td>
<td>Enables traffic shaping and configures traffic shaping parameters</td>
<td>page 7-417</td>
</tr>
<tr>
<td>trustpoint (profile-config-mode)</td>
<td>Configures the trustpoint assigned for validating a CMP auth Operator</td>
<td>page 7-422</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Configures the name of tunneled WLAN (extended VLAN) wireless controller or service platform</td>
<td>page 7-424</td>
</tr>
<tr>
<td>use</td>
<td>Uses pre configured policies with this profile</td>
<td>page 7-425</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configures Virtual Router Redundancy Protocol (VRRP) group settings</td>
<td>page 7-430</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>Publishes interface via OSPF or BGP based on VRRP status</td>
<td>page 7-434</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enables support for 802.11 WEP shared key authentication</td>
<td>page 7-438</td>
</tr>
<tr>
<td>service</td>
<td>Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode</td>
<td>page 7-436</td>
</tr>
<tr>
<td>slot</td>
<td>Assigns a physical slot for running Team-Centro VM on this profile/device. This feature is support only on the NX45XX and NX65XX series service platforms.</td>
<td>page 7-441</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
7.1.1 adopter-auto-provisioning-policy-lookup

Profile Config Commands

Enables the use of a centralized auto provisioning policy on this profile or device. This option is applicable in a hierarchically managed (HM) network. When enabled, the auto-provisioning policy applied on the NOC gets precedence over the one applied at the site controller level. Optionally, use the ‘evaluate-always’ option to set flag to run centralized auto-provisioning policy every time a device (access point/controller) is adopted. The device’s previous adoption status is not taken into consideration.

When applied on devices adopted by a controller, this profile allows the devices to use a centralized auto provisioning policy.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

adopter-auto-provisioning-policy-lookup {evaluate-always}

Parameters

- adopter-auto-provisioning-policy-lookup {evaluate-always}

Examples

rfs7000-6DCD4B(config-profile-default-rfs7000)#adopter-auto-provisioning-policy-lookup evaluate-always

rfs7000-6DCD4B(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000 autoinstall configuration autoinstall firmware crypto ikev1 policy ikev1-default isakmp-proposal default encryption aes-256 group 2 hash sha crypto ikev2 policy ikev2-default isakmp-proposal default encryption aes-256 group 2 hash sha crypto ipsec transform-set default esp-aes-256 esp-sha-hmac crypto ikev1 remote-vpn crypto ikev2 remote-vpn crypto auto-ipsec-secure crypto remote-vpn-client interface mel interface gel interface ge2 interface ge3 interface ge4 interface pppoe1 use firewall-policy default service pm sys-restart 

adopter-auto-provisioning-policy-lookup evaluate-always 

router ospf

rfs7000-6DCD4B(config-profile-default-rfs7000)#

Related Commands

no | Disables the application of centralized auto provisioning policy on this profile or device
7.1.2 adoption

Profile Config Commands

Configures a minimum and maximum delay time in the initiation of the device adoption process. When configured, devices do not attempt adoption immediately on coming up. The process is initiated after the lapse of a specified period of time (configured using this command as the start-delay minimum time).

Once configured and applied, this setting is applicable on all devices using this profile. This option is also available in the device-configuration mode.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
adoption start-delay min <0-30> max <0-30>

Parameters
- adoption start-delay min <0-30> max <0-30>

Examples
rfs7000-6DCD4B(config-profile-default-rfs7000)#adoption start-delay min 10 max 30
rfs7000-6DCD4B(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  autoinstall configuration
  autoinstall firmware
  crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  .................................................................
  interface ge2
  interface ge3
  interface ge4
  interface pppoe1
  use firewall-policy default
  service pm sys-restart
  adopter-auto-provisioning-policy-lookup evaluate-always
  router ospf
  adoption start-delay min 10 max 30
rfs7000-6DCD4B(config-profile-default-rfs7000)#

Related Commands

no

Removes the configured minimum start-delay value. When removed, devices attempt adoption immediately on coming up.
### 7.1.3 alias

**Profile Config Commands**

Configures network, VLAN, and service aliases. The aliases defined on this profile applies to all devices using this profile. Aliases can be also defined at the device level.

---

**NOTE:** You can apply overrides to aliases at the device level. For more information on aliases, see `alias`. Overrides applied at the device level take precedence.

---

**Supported in the following platforms:**

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX9000, NX9500, NX9510, NX9600

**Syntax**

- `alias [address-range|host|network|network-group|network-service|number|string|vlan]`
- `alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>`
- `alias host <HOST-ALIAS-NAME> <HOST-IP>`
- `alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>`
- `alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]`
- `alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP>] [host <HOST-IP> [<HOST-IP>]] [network <NETWORK-ADDRESS/MASK> [<NETWORK-ADDRESS/MASK>]]`
- `alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www}]
- `alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport <1-65535>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<WORD>|<W
### Parameters

- alias address-range `<ADDRESS-RANGE-ALIAS-NAME>` `<STARTING-IP>` to `<ENDING-IP>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ADDRESS-RANGE-ALIAS-NAME&gt;</code></td>
<td>Creates a new address-range alias for this profile. Or associates an existing address-range alias with this profile. An address-range alias maps a name to a range of IP addresses. Use this option to create unique address-range aliases for different deployment scenarios. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location’s network range is 172.16.13.20 through 172.16.13.110, the remote location’s ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.</td>
</tr>
<tr>
<td><code>&lt;STARTING-IP&gt;</code> to <code>&lt;ENDING-IP&gt;</code></td>
<td>Associates a range of IP addresses with this address range alias</td>
</tr>
<tr>
<td><code>&lt;ADDRESS-RANGE-ALIAS-NAME&gt;</code></td>
<td>– Specify the address range alias name.</td>
</tr>
<tr>
<td><code>&lt;STARTING-IP&gt;</code></td>
<td>– Specify the first IP address in the range.</td>
</tr>
<tr>
<td><code>&lt;ENDING-IP&gt;</code></td>
<td>– Specify the last IP address in the range.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If using an existing address-range alias, you can apply overrides to the alias at the profile level.</td>
</tr>
</tbody>
</table>

- alias host `<HOST-ALIAS-NAME>` `<HOST-IP>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;HOST-ALIAS-NAME&gt;</code></td>
<td>Creates a new host alias for this profile. Or associates an existing host alias with this profile. A host alias configuration is for a particular host device’s IP address. Use this option to create unique host aliases for different deployment scenarios. For example, if a central network DNS server is set a static IP address, and a remote location’s local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.</td>
</tr>
<tr>
<td><code>&lt;HOST-IP&gt;</code></td>
<td>Associates the network host’s IP address with this host alias</td>
</tr>
<tr>
<td><code>&lt;HOST-ALIAS-NAME&gt;</code></td>
<td>– Specify the host alias name.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Alias name should begin with ‘$’.</td>
</tr>
</tbody>
</table>

- alias network `<NETWORK-ALIAS-NAME>` `<NETWORK-ADDRESS/MASK>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;NETWORK-ALIAS-NAME&gt;</code></td>
<td>Creates a new network alias for this profile. Or associates an existing network alias with this profile. A network alias configuration is utilized for an IP address on a particular network. Use this option to create unique Network aliases for different deployment scenarios. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location’s network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-ADDRESS/MASK&gt;</code></td>
<td>– Specify the network alias name.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Alias name should begin with ‘$’.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `<NETWORK-ADDRESS/MASK>` | Associates a single network with this network alias  
  • `<NETWORK-ADDRESS/MASK>` – Specify the network’s address and mask.  
  **Note:** If using an existing network alias, you can apply overrides to the alias at the profile level. |
| `network <NETWORK-GROUP-ALIAS-NAME>` | Creates a new network-group alias for this profile. Or associates an existing network-group alias with this profile.  
  • `<NETWORK-GROUP-ALIAS-NAME>` – Specify the network-group alias name.  
  **Note:** Alias name should begin with `$`.  
  **Note:** The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level.  
  After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.  
  **Note:** If using an existing network-group alias, you can apply overrides to the alias at the profile level. |
| `address-range <STARTING-IP> to <ENDING-IP>` {<STARTING-IP> to <ENDING-IP>}` | Associates a range of IP addresses with this network-group alias  
  • `<STARTING-IP>` – Specify the first IP address in the range.  
  • to `<ENDING-IP>` – Specify the last IP address in the range.  
  • `<STARTING-IP>` to `<ENDING-IP>` – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured. |
| `host <HOST-IP>` {<HOST-IP>}` | Associates a single or multiple hosts with this network-group alias  
  • `<HOST-IP>` – Specify the hosts’ IP address.  
  • `<HOST-IP>` – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured. |
| `network <NETWORK-ADDRESS/MASK>` {<NETWORK-ADDRESS/MASK>}` | Associates a single or multiple networks with this network-group alias  
  • `<NETWORK-ADDRESS/MASK>` – Specify the network’s address and mask.  
  • `<NETWORK-ADDRESS/MASK>` – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured. |
| `alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntpxpop3|proto|sip|smtp|sourceport [<1-65535]|<WORD>|ssh|telnet|tftp|www})` | Creates a new network-service alias for this profile. Or associates an existing network-service alias with this profile. A network service alias is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.  
  • `<NETWORK-SERVICE-ALIAS-NAME>` – Specify a network-service alias name.  
  **Note:** Alias name should begin with `$`.  
  **Note:** The network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level.  
  **Note:** If using an existing network-service alias, you can apply overrides to the alias at the profile level. |
proto \[<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp]\]

Use one of the following options to associate an Internet protocol with this network-service alias:

- <0-254> – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the Protocol field of the IPv4 header and the Next Header field of IPv6 header. For example, the User Datagram Protocol’s (UDP) designated number is 17.
- <WORD> – Identifies the protocol by its name. Specify the protocol name.
- gre – Selects Generic Routing Encapsulation (GRE). The protocol number is 47.
- igmp – Selects Internet Group Management Protocol (IGMP). The protocol number is 2.
- ospf – Selects Open Shortest Path First (OSPF). The protocol number is 89.
- vrrp – Selects Virtual Router Redundancy Protocol (VRRP). The protocol number is 112.

\{(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport\[<1-65535>|<WORD>|ssh|telnet|tftp|www}\}

After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.

- <1-65535> – Optional. Configures a destination port number from 1 - 65535.
- <WORD> – Optional. Identifies the destination port by the service name provided. For example, the secure shell (SSH) service uses TCP port 22.
- bgp – Optional. Configures the default Border Gateway Protocol (BGP) services port (179).
- dns – Optional. Configures the default Domain Name System (DNS) services port (53).
- ftp – Optional. Configures the default File Transfer Protocol (FTP) control services port (21).
- ftp-data – Optional. Configures the default FTP data services port (20).
- gopher – Optional. Configures the default gopher services port (70).
- https – Optional. Configures the default HTTPS services port (443).
- nntp – Optional. Configures the default Newsgroup (NNTP) services port (119).
- ntp – Optional. Configures the default Network Time Protocol (NTP) services port (123).
- proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.
- pop3 – Optional. Configures the default Post Office Protocol (POP3) services port (110).
- smtp – Optional. Configures the default Simple Mail Transfer Protocol (SMTP) services port (25).
- sip – Optional. Configures the default Session Initiation Protocol (SIP) services port (5060).
- sourceport \[<1-65535>|<WORD>\] – Optional. After specifying the destination port, you may specify a single or range of source ports.
  - <1-65535> – Specify the source port from 1 - 65535.
  - <WORD> – Specify the source port range, for example 1-10.

Contd..
- **ssh** – Optional. Configures the default SSH services port (22)
- **telnet** – Optional. Configures the default Telnet services port (23)
- **tftp** – Optional. Configures the default *Trivial File Transfer Protocol* (TFTP) services port (69)
- **www** – Optional. Configures the default HTTP services port (80)

**alias number** `<NUMBER-ALIAS-NAME>` `<0-4294967295>`

Creates a number alias identified by the `<NUMBER-ALIAS-NAME>` keyword. Number aliases map a name to a numeric value. For example, ‘alias number $NUMBER 100’

- The number alias name is: $NUMBER
- The value assigned is: 100

The value referenced by alias $NUMBER, wherever used, is 100.

- `<NUMBER-ALIAS-NAME>` – Specify the number alias name.
- `<0-4294967295>` – Specify the number, from 0 - 4294967295, assigned to the number alias created.

**Note:** Alias name should begin with ‘$’.

**alias string** `<STRING-ALIAS-NAME>` `<LINE>`

Creates a new string alias for this profile. Or associates an existing string alias with this profile. String aliases map a name to an arbitrary string value. Use this option to create unique string aliases for different deployment scenarios. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

- `<STRING-ALIAS-NAME>` – Specify the string alias name.
- `<LINE>` – Specify the string value.

**Note:** Alias name should begin with ‘$’.

**Note:** If using an existing string alias, you can apply overrides to the alias at the RF Domain level.

**alias vlan** `<VLAN-ALIAS-NAME>` `<1-4094>`

Creates a new VLAN alias for this profile. Or associates an existing VLAN alias with this profile. A VLAN alias maps a name to a VLAN ID. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. Use this option to create unique VLAN aliases for different deployment scenarios. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

- `<VLAN-ALIAS-NAME>` – Specify the VLAN alias name.

**Note:** Alias name should begin with ‘$’.

- `<1-4094>` Maps the VLAN alias to a VLAN ID
  - `<1-4094>` – Specify the VLAN ID from 1 - 4094.

**Note:** If using an existing VLAN alias, you can apply overrides to the alias at the profile level.
Examples

The following example shows the global aliases configured. Note the network-service alias '$kerberos' settings.

```bash
rfs4000-229D58(config)#show context
!
Configuration of RFS4000 version 5.8.1.0-025D
!
!
version 2.3
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias network-service $kerberos proto tcp 749 750 80 proto udp 68 sourceport 67
!
alias vlan $TestVLANAlias 1
--More--
rfs4000-229D58(config)#
```

The following examples show the overrides applied to the network-service alias '$kerberos' at the profile level:

```bash
rfs4000-229D58(config-profile-TestRFS4000)#alias network-service $kerberos proto tcp 88 proto udp 80
rfs4000-229D58(config-profile-TestRFS4000)#
```

The following example shows the overrides applied to the network-service alias '$kerberos' at the profile level:

```bash
rfs4000-229D58(config-profile-TestRFS4000)#show context
profile rfs4000 TestRFS4000
no autoinstall configuration
no autoinstall firmware
...........................

service pm sys-restart
router ospf
alias network-service $kerberos proto tcp 88 proto udp 80
rfs4000-229D58(config-profile-TestRFS4000)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the use of centralized auto provisioning policy on this profile or device</td>
</tr>
</tbody>
</table>
7.1.4 application-policy

**Profile Config Commands**

Associates a RADIUS server provided application policy with this profile. This command is also applicable to the device configuration mode. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane.

Supported in the following platforms:
- Access Points — AP7522, AP7532, AP7562
- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

```
application-policy radius <APP-POLICY-NAME>
```

**Parameters**

- `application-policy radius <APP-POLICY-NAME>`

**Examples**

```
nx9500-6C8809(config)#show context include-factory | include application-policy

application-policy Bing
  no use application-policy
  no use application-policy
  no use application-policy
  no use application-policy
  no use application-policy
  no use application-policy
  no use application-policy
  no use application-policy

nx9500-6C8809(config-profile-testNX9000)#application-policy radius Bing

nx9500-6C8809(config-profile-testNX9000)#show context include-factory | include application-policy

application-policy radius Bing

nx9500-6C8809(config-application-Bing)#Show context

application Bing
  app-category streaming
  use url-list Bing
```

**Related Commands**

```
no
```

Removes the RADIUS-server provided application policy associated with this profile.
### 7.1.5 area

- **Profile Config Commands**

Sets the system's area of location (the physical area of deployment)

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
area <WORD>
```

**Parameters**

- `<WORD>`

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)# area Ecospace
rfs7000-37FABE(config-profile-default-rfs7000)# show context
```

**Related Commands**

- **no** Resets the configured area name

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area <code>&lt;WORD&gt;</code></td>
<td>Sets the system's area of location</td>
</tr>
<tr>
<td><code>&lt;WORD&gt;</code></td>
<td>Specify the area name (should not exceed 64 characters)</td>
</tr>
</tbody>
</table>

---

`--More--`

```
rfs7000-37FABE(config-profile-default-rfs7000)#
```
7.1.6 arp

Profile Config Commands

Adds a static Address Resolution Protocol (ARP) IP address in the ARP cache.

The ARP protocol maps an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP finds a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length, formatted, and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to locate a device that recognizes the IP address. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
arp [<IP>|timeout]
```

```
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial <1-4> <1-1> <1-1> [dhcp-server|router]
```

```
arps timeout <15-86400>
```

Parameters

- **arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial <1-4> <1-1> <1-1> [dhcp-server|router]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp &lt;IP&gt;</td>
<td>Adds a static ARP IPv4 address in the ARP cache.</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Specify the MAC address associated with the IP and the Switch Virtual Interface (SVI).</td>
</tr>
<tr>
<td>arpa</td>
<td>Sets ARP encapsulation type to ARPA.</td>
</tr>
<tr>
<td>&lt;L3-INTERFACE-NAME&gt;</td>
<td>Configures static ARP entry for a specified router interface.</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Configures static ARP entry for PPP over Ethernet interface.</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Configures static ARP entry for a VLAN interface.</td>
</tr>
<tr>
<td>wwan1</td>
<td>Configures static ARP entry for Wireless WAN interface.</td>
</tr>
</tbody>
</table>
### serial <1-4> <1-1> <1-1>

Configures the static ARP entry for serial interface

- **<1-4>** – Specify the Slot ID
- **<1-1>** – Specify the port ID.
- **<1-1>** – Specify the Channel group ID.

The serial interface is applicable for the NX45XX and NX65XX series service platforms only.

### {dhcp-server|router}

The following keywords are common to all of the above interface types:

- dhcp-server – Optional. Sets ARP entries for a DHCP server
- router – Optional. Sets ARP entries for a router

### arp timeout <15-86400>

Sets ARP entry timeout

- **<TIME>** – Sets the ARP entry timeout in seconds. Specify a value from 15 - 86400 seconds. The default is 3600 seconds.

### Examples

rfs7000-37FABE(config-profile-default-rfs7000)#arp timeout 2000

rfs7000-37FABE(config-profile-default-rfs7000)#show context

profile rfs7000 default-rfs7000
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  **arp timeout 2000**
  crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
  interface mel
  interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  interface ge2
  ip dhcp trust
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#

### Related Commands

| no | Removes an entry from the ARP cache |
7.1.7 auto-learn-staging-config

Profile Config Commands

Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

auto-learn-staging-config

Parameters

None

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#auto-learn-staging-config
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables automatic recognition of devices pending adoption</td>
</tr>
</tbody>
</table>
7.1.8 **autogen-uniqueid**

> **Profile Config Commands**

Autogenerates a unique ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device.

A device’s unique ID is a combination of a user-defined string (prefix, suffix, or both) and a substitution token. The WiNG implementation provides two built-in substitution tokens: $SN and $MiNT-ID that represent the device’s serial number and MiNT-ID respectively. The value referenced by these substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for the device.

The general format of this command is: `<PREFIX><SUBSTITUTION-TOKEN><SUFFIX>`. You can provide both (prefix and suffix) or just a prefix or suffix.

For example, given the following set of inputs:
- user-defined prefix – TestAP6522
- substitution token – $SN

The unique ID is generated using TestAP6522$SN, where $SN is replaced with the device’s serial number.

When executed on an AP6522 (having serial number B4C7996C8809), the autogen-uniqueid TestAP6522$SN command generates the unique ID: TestAP6522B4C7996C8809. When configured on an AP6522 profile, all AP6522s using the profile autogenerate a unique ID in which the device’s serial number is preceded by the string ‘TestAP6522’.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`autogen-uniqueid <WORD>`

**Parameters**

- `autogen-uniqueid <WORD>`

| autogen-uniqueid <WORD> | Autogenerates a device’s unique ID (not exceeding 64 characters in length) The ID generated is a combination of the text provided and the value referenced through the substitution token $SN or $MiNT-ID. Where ever the autogen-uniqueid is used the device’s serial number OR MiNT-ID is referenced depending on the substitution token used.
| | • `<WORD>` – Specify a auto generate unique ID format using one of the following substitution tokens:
| | | Available tokens:
| | | $SN     - references SERIAL NUMBER of the device
| | | $MiNT-ID - references MiNT-ID of the device
| | For example, Test-$SN-TechPubs. In this example ‘Test’ and ‘TechPubs’ represent the user-defined prefix and suffix respectively. And $SN is the substitution token. |
Examples

```bash
nx4500-5CFA2B(config-profile-testAP6522)#autogen-uniqueid TestAP6522$SN

nx4500-5CFA2B(config-profile-testAP6522)#show context
profile ap621 testAP621
  autogen-uniqueid TestAP6522$SN
  no autoinstall configuration
  no autoinstall firmware
  interface radio1
  interface ge1
  use firewall-policy default
  service pm sys-restart

nx4500-5CFA2B(config-profile-testAP6522)#

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#autogen-uniqueid Test-$MiNT-ID-TechPubs

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#show context
nx45xx B4-C7-99-5C-FA-2B
  use profile default-nx45xx
  use rf-domain default
  hostname nx4500-5CFA2B
  license AP DEFAULT-12AP-LICENSE
  license ADSEC DEFAULT-ADV-SEC-LICENSE
  environmental-sensor temperature
  autogen-uniqueid Test-$MiNT-ID-TechPubs
  ip default-gateway 192.168.13.2
  interface up1
    no shutdown
    switchport mode access
    switchport access vlan 1
  interface vlan1
    ip address 192.168.13.12/24
  logging on
  logging console warnings
  logging buffered warnings

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>When executed in the device configuration mode, removes the device’s autogen-uniqueid. When executed in the profile configuration mode, removes the autogen-uniqueid on all devices using the profile.</td>
</tr>
</tbody>
</table>
7.1.9 autoinstall

Profile Config Commands

Automatically installs firmware image and startup configuration parameters on to the selected device.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

autoinstall [configuration|firmware|start-interval <WORD>]

Parameters

- autoinstall [configuration|firmware|start-interval <WORD>]

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Autoinstalls startup configuration. Setup parameters are automatically configured on devices using this profile. This option is disabled by default.</td>
</tr>
<tr>
<td>firmware</td>
<td>Autoinstalls firmware image. Firmware images are automatically installed on devices using this profile. This option is disabled by default.</td>
</tr>
<tr>
<td>start-interval &lt;WORD&gt;</td>
<td>Configures the interval between system boot and start of autoinstall process (this is the time, from system boot, after which autoinstall should start)</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the interval in minutes. The default is 10.</td>
</tr>
</tbody>
</table>

Note: Zero (0) implies firmware or startup configuration installation can start any time.

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#autoinstall configuration
rfs7000-37FABE(config-profile-default-rfs7000)#autoinstall firmware
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  arp timeout 2000
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface mel
interface gel
  ip dhcp trust
  --More--
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the auto install settings</td>
</tr>
</tbody>
</table>
### 7.1.10 bluetooth-detection

**Profile Config Commands**

Enables detection of Bluetooth devices. These are devices using the Bluetooth USB module.

When enabled, the access point scans for Bluetooth devices over the WiNG managed 2.4 GHz access point radio. Bluetooth is a technology for exchanging data over short distances using short-wavelength UHF radio waves in the 2.4 GHz band from mobile wireless clients.

---

**NOTE:** Enabling Bluetooth detection results in interference on the access point's 2.4 GHz radio when in WLAN mode. WLANs are susceptible to sources of interference by Bluetooth devices.

---

Supported in the following platforms:
- Access Points — AP81XX

**Syntax**

```
bluetooth-detection
```

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile-default-ap81xx)#bluetooth-detection
```

```
nx9500-6C8809(config-profile-default-ap81xx)#show context
profile ap81xx default-ap81xx
no autoinstall configuration
no autoinstall firmware
crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
    crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
    crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radio1
interface radio2
interface radio3
interface gel
interface ge2
interface wwan1
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
    bluetooth-detection
nx9500-6C8809(config-profile-default-ap81xx)#
```

**Related Commands**

| no | Enables detection of Bluetooth devices on this profile. Devices using this profile are not bluetooth-detection enabled. |
The following table summarizes Ethernet bridge configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge</td>
<td>Enables Ethernet bridge configuration context</td>
<td>page 7-30</td>
</tr>
<tr>
<td>bridge-vlan-mode commands</td>
<td>Summarizes bridge VLAN configuration mode commands</td>
<td>page 7-33</td>
</tr>
</tbody>
</table>
7.1.11.1 bridge

Bridge configurations VLAN Ethernet bridging parameters. Use this command to configure a Bridge NAT or Bridge VLAN settings.

Configuring bridge Network Address Translation (NAT) parameters, allows management of Internet traffic originating at a remote site. In addition to traditional NAT functionality, bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router. Using bridge NAT, a tunneled VLAN (extended VLAN) is created between the NOC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NOC, and from there routed to the Internet. This increases the access time for the end user on the client. To resolve latency issues, bridge NAT identifies and segregates traffic heading towards the NOC and outwards towards the Internet. Traffic towards the NOC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

A Virtual LAN (VLAN) is a separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined within wireless controllers or service platforms to allow control of broadcast, multicast, unicast, and unknown unicast within a layer 2 device. For example, say several computers are used in conference room X and some in conference Y. The systems in conference room X can communicate with one another, but not with the systems in conference room Y. The VLAN enables the systems in conference rooms X and Y to communicate with one another even though they are on separate physical subnets. The systems in conference rooms X and Y are managed by the same single wireless controller or service platform, but ignore the systems that are not using the same VLAN ID. Administrators often need to route traffic between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device, which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the bridge VLAN forwards the data frame on the appropriate port(s). VLANs are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers can do this on their own, without need for the computer or other gear to know itself what VLAN it is on (this is called port-based VLAN, since it is assigned by port of the switch). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or quality of service.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Switch Note: For more information on the interface types and the devices supporting them, see interface.

Syntax

bridge [nat|vlan]

bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface
  [<LAYER3-INTERFACE-NAME>|pppoel|vlan <1-4094>|wwan1] [{(address|interface|overload|pool <NAT-POOL-NAME>)}]

bridge vlan [<1-4094>|<VLAN-ALIAS-NAME>]
**Parameters**

- `bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface [<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address|interface|overload|pool <NAT-POOL-NAME>)]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nat</code></td>
<td>Configures bridge NAT parameters</td>
</tr>
<tr>
<td><code>source</code></td>
<td>Configures NAT source addresses</td>
</tr>
<tr>
<td><code>list</code></td>
<td>Associates an access control list (ACL) with this bridge NAT policy. The ACL specifies the IP address permit/deny rules applicable to this bridge NAT policy.</td>
</tr>
<tr>
<td><code>&lt;IP-ACCESS-LIST-NAME&gt;</code></td>
<td>Specify access list name.</td>
</tr>
<tr>
<td><code>precedence &lt;1-500&gt;</code></td>
<td>Specifies a precedence value for this bridge NAT policy.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Selects one of the following as the primary interface (between the source and destination points):</td>
</tr>
<tr>
<td><code>&lt;LAYER3-INTERFACE-NAME&gt;</code></td>
<td>A router interface. Specify interface name.</td>
</tr>
<tr>
<td><code>pppoe1</code></td>
<td>A PPP over Ethernet interface.</td>
</tr>
<tr>
<td><code>vlan &lt;1-4094&gt;</code></td>
<td>A VLAN interface. Specify the VLAN interface index from 1-4094.</td>
</tr>
<tr>
<td><code>wwan1</code></td>
<td>A Wireless WAN interface.</td>
</tr>
<tr>
<td>`[(address</td>
<td>interface</td>
</tr>
<tr>
<td><code>address</code></td>
<td>Configures the interface IP address used for NAT</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Configures the failover interface (default setting)</td>
</tr>
<tr>
<td><code>overload</code></td>
<td>Enables use of one global address for multiple local addresses (terminates command)</td>
</tr>
<tr>
<td><code>pool &lt;NAT-POOLNAME&gt;</code></td>
<td>Configures the NAT pool used with this bridge NAT policy. Specify the NAT pool name. For more information on configuring a NAT pool, see <code>nat-pool-config-instance</code>.</td>
</tr>
<tr>
<td><code>vlan &lt;1-4094&gt;</code></td>
<td>Configures the numerical identifier for the Bridge VLAN when it was initially created.</td>
</tr>
<tr>
<td><code>&lt;1-4094&gt;</code></td>
<td>Specify a VLAN index from 1-4094.</td>
</tr>
<tr>
<td><code>vlan &lt;VLAN-ALIAS-NAME&gt;</code></td>
<td>Configures the VLAN alias (should be existing and configured) identifying the bridge VLAN</td>
</tr>
<tr>
<td><code>&lt;VLAN-ALIAS-NAME&gt;</code></td>
<td>Specify a VLAN alias name.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment.

If a bridge does not hear *Bridge Protocol Data Units* (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.
Examples

rfs7000-37FABE(config-profile-default-rfs7000)#bridge vlan 1
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#?

Bridge VLAN Mode commands:
- **bridging-mode**: Configure how packets on this VLAN are bridged
- **captive-portal**: Captive Portal
- **description**: Vlan description
- **edge-vlan**: Enable edge-VLAN mode
- **firewall**: Enable vlan firewall (IPv4)
- **http-analyze**: Forward URL and Data to controller
- **ip**: Internet Protocol (IP)
- **ipv6**: Internet Protocol version 6 (IPv6)
- **l2-tunnel-broadcast-optimization**: Enable broadcast optimization
- **no**: Negate a command or set its defaults
- **stateful-packet-inspection-l2**: Enable stateful packet inspection in layer2 firewall
- **tunnel**: Vlan tunneling settings
- **tunnel-over-level2**: Tunnel extended VLAN traffic over level 2 MiNT links
- **use**: Set setting to use
- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **do**: Run commands from Exec mode
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
bridge-vlan-mode commands

The following table summarizes bridge VLAN configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging-mode</td>
<td>Configures how packets on this VLAN are bridged</td>
<td>page 7-34</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Enables IP packet snooping on wired captive portals, and also</td>
<td>page 7-35</td>
</tr>
<tr>
<td></td>
<td>configures the subnet to snoop</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>Configures VLAN bridge description</td>
<td>page 7-36</td>
</tr>
<tr>
<td>edge-vlan</td>
<td>Enables edge VLAN mode</td>
<td>page 7-37</td>
</tr>
<tr>
<td>firewall</td>
<td>Enables firewall on this bridge VLAN interface</td>
<td>page 7-38</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enables the analysis of URLs and data traffic on this Bridge VLAN</td>
<td>page 7-39</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP components</td>
<td>page 7-40</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures IPv6 components</td>
<td>page 7-43</td>
</tr>
<tr>
<td>l2-tunnel-broadcast-optimization</td>
<td>Enables broadcast optimization</td>
<td>page 7-46</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 7-47</td>
</tr>
<tr>
<td>stateful-packet-inspection-l2</td>
<td>Enables statedly packet inspection in the layer 2 fire wall</td>
<td>page 7-49</td>
</tr>
<tr>
<td>tunnel</td>
<td>Enables tunneling of unicast messages to unknown MAC destinations,</td>
<td>page 7-50</td>
</tr>
<tr>
<td></td>
<td>on the selected VLAN bridge</td>
<td></td>
</tr>
<tr>
<td>tunnel-over-level2</td>
<td>Enables extended VLAN traffic over level 2 MiNT links</td>
<td>page 7-52</td>
</tr>
<tr>
<td>use</td>
<td>Associates a captive-portal, access control list (IP, IPv6, or MAC), and</td>
<td>page 7-53</td>
</tr>
<tr>
<td></td>
<td>a URL filter with this bridge VLAN</td>
<td></td>
</tr>
</tbody>
</table>
### 7.1.11.2.1 bridging-mode

**bridge-vlan-mode commands**

Configures how packets are bridged on the selected VLAN

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

**Parameters**

- **bridging-mode [auto|isolated-tunnel|local|tunnel]**

<table>
<thead>
<tr>
<th>bridging-mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Automatically selects the bridging mode to match the WLAN, VLAN and bridging mode configurations. When selected, the controller or access point determines the best bridging mode for the VLAN. (default setting)</td>
</tr>
<tr>
<td>isolated-tunnel</td>
<td>Bridges packets between local Ethernet ports and local radios, and passes tunneled packets through without de-tunneling. Select this option for a dedicated tunnel for bridging VLAN traffic.</td>
</tr>
<tr>
<td>local</td>
<td>Bridges packets normally between local Ethernet ports and local radios (if any). Local mode is typically configured in remote branch offices where traffic on remote private LAN segments need to be bridged locally. Local mode implies that traffic, wired and wireless, is to be bridged locally.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Bridges packets between local Ethernet ports, local radios, and tunnels to other APs, wireless controllers, or service platforms. Select this option to use a shared tunnel for bridging VLAN traffic. In tunnel mode, the traffic at the AP is always forwarded through the best path. The APs decide the best path to reach the destination and forward packets accordingly. Setting the VLAN to tunnel mode ensures packets are bridged between local Ethernet ports, any local radios, and tunnels to other APs, wireless controllers, and service platforms.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#bridging-mode isolated-tunnel
```

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context bridge vlan 1 bridging-mode isolated-tunnel ip igmp snooping ip igmp snooping querier
```

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

**Related Commands**

- **no** Resets bridging mode to auto
7.11.2.2 captive-portal

*bridge-vlan-mode commands*

Enables IP packet snooping on wired captive portals, and also configures the subnet to snoop. When enabled, IP packets received from wired captive portal clients, on the specified subnet, are snooped to learn IP to MAC mapping.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controller
- Access Points — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

captive-portal [ipv4-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M>
{excluded-address <IPv4|IPv6>}

**Parameters**

- captive-portal [ipv4-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M> {excluded-address <IPv4|IPv6>}

| captive-portal [ipv4-snooping|ipv6-snooping] | Enables snooping of IPv4 or IPv6 packets (based on the option selected) for wired captive portal clients |
| subnet <IPv4/M|IPv6/M> | Enables IPv4 or IPv6 packet snooping on a specified subnet
- <IPv4/M|IPv6/M> – Specify the subnet address in the A.B.C.D/M or X:X::X:X/M format to identify an IPv4 or IPv6 subnet respectively. |
| excluded-address <IPv4|IPv6> | Optional. Configures the IPv4 or IPv6 address excluded from snooping
- <IPv4|IPv6> – Specify the IPv4 or IPv6 address. Use this parameter to configure the gateway’s address. |

**Examples**

```plaintext	nx9500-6C8809(config-profile NX9000Test-bridge-vlan-4)#captive-portal ip-snooping subnet 192.168.13.0/24 excluded-address 192.168.13.7
	nx9500-6C8809(config-profile NX9000Test-bridge-vlan-4)#show context
bridge vlan 4
captive-portal ip-snooping subnet 192.168.13.0/24 excluded-address 192.168.13.7
ip igmp snooping
ip igmp snooping querier
ipv6 mld snooping
ipv6 mld snooping querier
nx9500-6C8809(config-profile NX9000Test-bridge-vlan-4)#
```

**Related Commands**

| no | Disables IP packet snooping on wired captive portals |
7.1.11.2.3 description

Configures VLAN bridge description

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

description <WORD>

Parameters
- <WORD> — Enter a description. The description should be unique to the VLAN’s specific configuration to help differentiate it from other VLANs with similar configurations.

Examples

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#description “This is a description for the bridged VLAN”

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
  bridge vlan 1
description This\ is\ a\ description\ for\ the\ bridged\ VLAN
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#

Related Commands

no

Removes VLAN bridge description
7.11.2.4 edge-vlan

*bridge-vlan-mode commands*

Enables the edge VLAN mode. In the edge VLAN mode, a protected port does not forward traffic to another protected port on the same wireless controller or service platform. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dedge-vlan

**Parameters**

None

**Examples**

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#edge-vlan
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the edge VLAN mode</td>
</tr>
</tbody>
</table>
7.1.12.5 firewall

*bridge-vlan-mode commands*

Enables IPv4 firewall on this bridge VLAN interface. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX5524, NX6500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`firewall`

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#firewall
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables firewall on this bridge VLAN interface</td>
</tr>
</tbody>
</table>
### 7.1.11.2.6 http-analyze

#### bridge-vlan-mode commands

Enables the analysis of URLs and data traffic on this Bridge VLAN. When enabled, URLs and data are forwarded to the controller running the HTTP analytics engine.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
http-analyze {filter [images|post|query-string]}
```

#### Parameters

- `http-analyze {filter [images|post|query-string]}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`http-analyze filter [images</td>
<td>post</td>
</tr>
<tr>
<td>- filter – Optional. Filters out specific URLs</td>
<td></td>
</tr>
<tr>
<td>- images – Filters out URLs referring to images</td>
<td></td>
</tr>
<tr>
<td>- post – Filters out URLs referring to POSTs</td>
<td></td>
</tr>
<tr>
<td>- query-string – Filters out query strings received from URLs</td>
<td></td>
</tr>
</tbody>
</table>

#### Examples

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#http-analyze filter images
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#show context bridge vlan 4
http-analyze filter images
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables forwarding of URLs and data to the controller running the HTTP analytics engine</td>
</tr>
</tbody>
</table>
### 7.1.11.2.7 ip

**bridge-vlan-mode commands**

Configures VLAN bridge IP components

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
ip [arp|dhcp|igmp]
ip [arp|dhcp] trust
ip igmp snooping {forward-unknown-multicast|mrouter|querier}
ip igmp snooping
{forward-unknown-multicast}
ip igmp snooping {mrouter [interface|learn]}
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}
ip igmp snooping {querier} {address|max-response-time|timer|version}
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|timer expiry <60-300>|version <1-3>}
```

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip [arp</td>
<td>dhcp] trust</td>
</tr>
<tr>
<td></td>
<td>- trust – Trusts ARP responses on the VLAN bridge</td>
</tr>
<tr>
<td>ip dhcp trust</td>
<td>Configures the DHCP trust parameter. Uses DHCP packets, from a DHCP server, as trusted and permissible within the access point, wireless controller, or service platform managed network. DHCP packets are used to update the DHCP snop table to prevent IP spoof attacks. This feature is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>- trust – Trusts DHCP responses on the VLAN bridge</td>
</tr>
<tr>
<td>ip igmp snooping {forward-unknown-multicast}</td>
<td>Configures Internet Group Management Protocol (IGMP) snooping parameters. IGMP snooping is enabled by default. IGMP establishes and maintains multicast group memberships for interested members. Multicasting allows a networked device to listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. The device also maintains a map of the links that require multicast streams, thereby reducing unnecessary flooding of the network with multicast traffic.</td>
</tr>
<tr>
<td>forward-unknown-multicast</td>
<td>Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is enabled by default.</td>
</tr>
</tbody>
</table>
- `ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Configures the VLAN bridge IP parameters</td>
</tr>
<tr>
<td>igmp snooping</td>
<td>Configures the IGMP snooping parameters</td>
</tr>
<tr>
<td>mrouter</td>
<td>Optional. Configures the multicast router parameters</td>
</tr>
<tr>
<td>interface &lt;INTERFACE-LIST&gt;</td>
<td>Configures the multicast router interfaces. This option is disabled by default.</td>
</tr>
<tr>
<td>learn pim-dvmrp</td>
<td>Configures the multicast router learning protocols. This option is disabled by default.</td>
</tr>
</tbody>
</table>

- `ip igmp snooping {querier} {address <IP>|max-response-time <1-25>| timer expiry <60-300>|version <1-3>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Configures the VLAN bridge IP parameters</td>
</tr>
<tr>
<td>igmp snooping</td>
<td>Configures the IGMP snooping parameters</td>
</tr>
<tr>
<td>querier</td>
<td>Optional. Configures the IGMP querier parameters. This option is disabled by default. Enables IGMP querier. IGMP snooping querier keeps host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The access point, wireless controller, or service platform performs the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.</td>
</tr>
<tr>
<td>address &lt;IP&gt;</td>
<td>Optional. Configures the IGMP querier source IP address. This address is used as the default VLAN querier IP address.</td>
</tr>
<tr>
<td>max-response-time &lt;1-25&gt;</td>
<td>Optional. Configures the IGMP querier maximum response time. This option is disabled by default.</td>
</tr>
<tr>
<td>timer expiry &lt;60-300&gt;</td>
<td>Optional. Configures the IGMP querier expiry time. The value specified is used as the timeout interval for other querier resources. This option is disabled by default.</td>
</tr>
<tr>
<td>version &lt;1-3&gt;</td>
<td>Optional. Configures the IGMP version. This option is disabled by default.</td>
</tr>
</tbody>
</table>

Protocol-Independent Multicast (PIM) and Distance-Vector Multicast Routing Protocol (DVMRP) snoping of packets
Examples
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip arp trust
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip dhcp trust
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping mrouter
interface ge1 ge2
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping mrouter
learn pim-dvmp
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping querier
max-response-time 24
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping querier
timer expiry 100
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#ip igmp snooping querier
version 2
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
bridge vlan 1
   description This\ is\ a\ description\ of\ the\ bridged\ VLAN
   ip arp trust
   ip dhcp trust
   ip igmp snooping
   ip igmp snooping querier
   ip igmp snooping querier version 2
   ip igmp snooping querier max-response-time 24
   ip igmp snooping querier timer expiry 100
   ip igmp snooping mrouter interface ge2 ge1
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts the VLAN Ethernet bridge parameters</td>
</tr>
</tbody>
</table>
7.1.11.2.8 ipv6

**bridge-vlan-mode commands**

Configures this VLAN bridge's IPv6 components

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ipv6 [dhcpv6|firewall|mld|nd]

ipv6 dhcpv6 trust
ipv6 firewall
ipv6 mld snooping {forward-unknown-multicast|mrouter|querier}
ipv6 mld snooping {forward-unknown-multicast}
ipv6 mld snooping {mrouterm [interface|learn]}
ipv6 mld snooping {mrouterm [interface INTERFACE-LIST]|learn pim-dvmrp}
ipv6 mld snooping {querier} {max-response-time|timer|version}
ipv6 mld snooping {querier} {max-response-time <1-25000>|timer expiry <60-300>}

ipv6 nd raguard

**Parameters**

- ipv6 dhcpv6 trust

  Configures the VLAN bridge IPv6 parameters
  dhcpv6 trust Enables the DHCPv6 trust option. When enabled all DHCPv6 responses are trusted on this bridge VLAN. This option is enabled by default.
  - trust – Trusts DHCPv6 responses on this bridge VLAN

- ipv6 firewall

  Configures the VLAN bridge IPv6 parameters
  firewall Enables IPv6 firewall on this bridge VLAN. This option is enabled by default. Devices utilizing IPv6 addressing require firewall protection unique to IPv6 traffic. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the **neighbor discovery** (ND) protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters. Routers respond to such a request with a **router advertisement** (RA) packet that contains Internet layer configuration parameters.
### ipv6 mld snooping \{forward-unknown-multicast\}

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Configures the VLAN bridge IPv6 parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>mld snooping</td>
<td>Configures Multicast Listener Discovery Protocol (MLD) snooping parameters. MLD snooping enables a access point, wireless controller, or service platform to examine MLD packets and make forwarding decisions based on the content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups. MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages between hosts and multicast routers are examined to identify the hosts receiving multicast group traffic. The access point, wireless controller, or service platform forward multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces. This option is enabled by default.</td>
</tr>
<tr>
<td>forward-unknown-multicast</td>
<td>Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is enabled by default.</td>
</tr>
</tbody>
</table>

### ipv6 mld snooping \{mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]\}

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Configures the VLAN bridge IPv6 parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>mld snooping</td>
<td>Configures MLD snooping parameters. This option is enabled by default.</td>
</tr>
<tr>
<td>mrouter</td>
<td>Optional. Configures the multicast router parameters, such as interfaces and learning protocol used.</td>
</tr>
<tr>
<td>interface &lt;INTERFACE-LIST&gt;</td>
<td>Configures the multicast router interfaces. This option is disabled by default.</td>
</tr>
<tr>
<td>learn pim-dvmrp</td>
<td>Configures the multicast router learning protocols. This option is disabled by default.</td>
</tr>
</tbody>
</table>

### ipv6 mld snooping \{querier\} \{max-response-time <1-25000>|timer expiry <60-300>\}

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Configures the VLAN bridge IPv6 parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>mld snooping</td>
<td>Configures IPv6 MLD snooping parameters. This option is disabled by default.</td>
</tr>
<tr>
<td>querier</td>
<td>Optional. Enables and configures the MLD querier parameters. When enabled, the device (access point, wireless controller, and service platform) sends query messages to discover which network devices are members of a given multicast group. This option is disabled by default.</td>
</tr>
<tr>
<td>max-response-time &lt;1-25000&gt;</td>
<td>Optional. Configures the IPv6 MLD querier’s maximum response time. This option is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-25000&gt; – Specify the maximum response time from 1 - 25000 milliseconds.</td>
</tr>
</tbody>
</table>
**ipv6 nd raguard**

- ipv6 nd raguard

| **timer expiry <60-300>** | Optional. Configures the IPv6 MLD other querier’s timeout. This option is disabled by default.
  - <60-300> – Specify the MLD other querier’s timeout from 60 - 300 seconds. |

| **version <1-2>** | Optional. Configures the IPv6 MLD querier version. This option is disabled by default.
  - <1-2> – Specify the MLD version. The versions are 1-2. |

**Examples**

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 dhcpv6 trust

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 firewall

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping forward-unknown-multicast

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping mrouter interface ge1 ge2

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping mrouter learn pim-dvmrp

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier max-response-time 20000

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier timer expiry 200

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier version 2

rfs7000-37FABE(config-profile test-bridge-vlan-2)#show context
  bridge vlan 2
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
  ipv6 mld snooping mrouter interface ge2 ge1
  ipv6 mld snooping querier version 2
  ipv6 mld snooping querier max-response-time 20000
  ipv6 mld snooping querier timer expiry 200
rfs7000-37FABE(config-profile test-bridge-vlan-2)#

**Related Commands**

| **no** | Disables or reverts the VLAN Ethernet bridge IPV6 parameters |
7.1.11.2.9 l2-tunnel-broadcast-optimization

▲ bridge-vlan-mode commands

Enables broadcast optimization on this bridge VLAN. Enabling this feature aids in the identification of each incoming packet. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
l2-tunnel-broadcast-optimization

Parameters
None

Examples
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#l2-tunnel-broadcast-optimization
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context bridge vlan 1
description This is a description for the bridged VLAN
l2-tunnel-broadcast-optimization
bridging-mode isolated-tunnel
ip arp trust
ip dhcp trust
ip igmp snooping
ip igmp snooping querier
ip igmp snooping mrouter interface ge2 ge1
ip igmp snooping querier version 2
ip igmp snooping querier max-response-time 24
ip igmp snooping querier timer expiry 100
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables broadcast optimization</td>
</tr>
</tbody>
</table>
7.1.11.2.10 no

**bridge-vlan-mode commands**

Negates a command or reverts settings to their default. The no command, when used in the bridge VLAN mode, negates the VLAN bridge settings or reverts them to their default.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [bridging-mode|captive-portal|description|edge-vlan|firewall|http-analyze|ip|ipv6|
    l2-tunnel-broadcast-optimization|stateful-packet-inspection-12|tunnel|
    tunnel-over-level2|use]
```

```
no [bridging-mode|description|edge-vlan|firewall|l2-tunnel-broadcast-optimization|
    stateful-packet-inspection-12|tunnel-over-level2]
```

```
no captive-portal [ip-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M>
    {excluded-address <IPv4|IPv6>}
```

```
no http-analyze {filter [images|post|query-string]}
```

```
no ip [arp|dhcp|igmp]
```

```
no ip [arp|dhcp] trust
```

```
no ip igmp snooping {forward-unknown-multicast|mrouter|querier}
```

```
no ip igmp snooping {forward-unknown-multicast}
```

```
no ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pin-dvmrp]}
```

```
no ip igmp snooping {querier} {address|max-response-time|timer expiry|version}
```

```
no ipv6 [dhcpv6|firewall|mld|nd]
```

```
no ipv6 dhcpv6 trust
```

```
no ipv6 firewall
```

```
no ipv6 mld snooping {forward-unknown-multicast}
```

```
no ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pin-dvmrp]}
```

```
no ipv6 mld snooping {querier} {max-response-time|timer expiry|version}
```

```
no ipv6 nd raguard
```

```
no tunnel [rate-limit level2|unknown-unicast]
```

```
no use [application-policy|captive-portal|ip-access-list|ipv6-access-list|
    mac-access-list|url-list] tunnel out
```

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Resets or reverts this bridge VLAN’s settings based on the parameters passed |

---
Examples

The following example displays bridge VLAN 20 settings before the ‘no’ commands are executed:

```
  nx4500-5CFA2B(config-profile default-nx45xx-bridge-vlan-20)#show context
  bridge vlan 20
    ip igmp snooping
    ip igmp snooping querier
    ipv6 mld snooping
    ipv6 mld snooping querier
  nx4500-5CFA2B(config-profile default-nx45xx-bridge-vlan-20)#
```

nx4500-5CFA2B(config-profile default-nx45xx-bridge-vlan-20)# no ip igmp snooping
nx4500-5CFA2B(config-profile default-nx45xx-bridge-vlan-20)# no ipv6 mld snooping querier

The following example displays bridge VLAN 20 settings after the ‘no’ commands are executed:

```
  nx4500-5CFA2B(config-profile default-nx45xx-bridge-vlan-20)#show context
  bridge vlan 20
    no ip igmp snooping
    no ip igmp snooping querier
    ipv6 mld snooping
    no ipv6 mld snooping querier
  nx4500-5CFA2B(config-profile default-nx45xx-bridge-vlan-20)#
```
7.1.11.2.11 stateful-packet-inspection-l2

- **bridge-vlan-mode commands**

  Enables a stateful packet inspection at the layer 2 firewall

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
stateful-packet-inspection-l2
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#stateful-packet-inspection-l2
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables stateful packet inspection at the layer 2 firewall</td>
</tr>
</tbody>
</table>
7.1.11.2.12 tunnel

*bridge-vlan-mode commands*

Enables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

tunnel [rate-limit|unknown-unicast]

tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024>
  {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}

tunnel unknown-unicast

**Parameters**
- **tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024>
  {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}**

<table>
<thead>
<tr>
<th>tunnel rate-limit level2</th>
<th>Configures a rate-limit parameters (max-burst-size and rate) for tunneled VLAN traffic over level 2 MiNT links</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate &lt;50-1000000&gt;</td>
<td>• rate – Optional. Configures the data rate, in kilobits per second, for the incoming and outgoing extended VLAN traffic tunneled over MiNT level 2 links</td>
</tr>
<tr>
<td>max-burst-size &lt;2-1024&gt;</td>
<td>• &lt;50-1000000&gt; – Specify a value from 50 - 1000000 Kbps. The default is 5000 Kbps.</td>
</tr>
<tr>
<td></td>
<td>• max-burst-size – Optional. Configures the maximum burst size</td>
</tr>
<tr>
<td></td>
<td>• &lt;2-1024&gt; – Specify the maximum burst size from 2 - 1024 kbytes. The default is 320 kbytes.</td>
</tr>
</tbody>
</table>

After specifying the max-burst-size, optionally specify the red-threshold value for the different traffic class. The red-threshold is configured as a % of the specified max-burst-size.

- red-threshold – Optional. Configures the random early detection threshold for the different traffic class
  - background – Configures the red-threshold for low priority traffic from 0 -100. The default is 50% of the specified max-burst-size.
  - best-effort – Configures the red-threshold for normal priority traffic from 0 -100. The default is 50% of the specified max-burst-size.
  - video – Configures the red-threshold for video traffic from 0 -100. The default is 25% of the specified max-burst-size.
  - voice – Configures the red-threshold for voice traffic from 0 -100. The default is 0% of the specified max-burst-size.

- **tunnel unknown-unicast**

| tunnel unknown-unicast | Enables tunneling of unicast packets destined for unknown MAC addresses |
Examples
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#tunnel unknown-unicast
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#no tunnel unknown-unicast
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#show context bridge vlan 1
ip igmp snooping
ip igmp snooping querier
no tunnel unknown-unicast
rfs7000-37FABE(config-profile TestAP81xx-bridge-vlan-1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge</td>
</tr>
</tbody>
</table>
7.111.2.13 tunnel-over-level2

▶ bridge-vlan-mode commands

Enables extended VLAN (tunneled VLAN) traffic over level 2 MiNT links. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
tunnel-over-level2

Parameters
None

Examples
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#tunnel-over-level2
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#show context
bridge vlan 1
description This is a test bridge VLAN
l2-tunnel-broadcast-optimization
bridging-mode isolated-tunnel
tunnel-over-level2
ip arp trust
ip dhcp trust
ip igmp snooping
ip igmp snooping querier
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#

Related Commands

no

Disables extended VLAN traffic over level 2 MiNT links
### 7.1.11.2.14 `use`

**bridge-vlan-mode commands**

Associates a captive-portal, access control list (IPv4, IPv6, or MAC), and/or a URL filter with this bridge VLAN

**Supported in the following platforms:**

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use [application-policy|captive-portal|ip-access-list|ipv6-access-list|mac-access-list|url-filter]
```

- `use application-policy <APP-POLICY-NAME>`
- `use captive-portal <CAPTIVE-PORTAL-NAME>`
- `use [ip-access-list|ipv6-access-list|mac-access-list] tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME>`
- `use url-filter <URL-FILTER-NAME>`

**Parameters**

- **use application-policy <APP-POLICY-NAME>**
  
<table>
<thead>
<tr>
<th><strong>use application-policy &lt;APP-POLICY-NAME&gt;</strong></th>
<th>Enforces application detection on this VLAN bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;APP-POLICY-NAME&gt;</code> – Specify the application policy name (should be existing and configured).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For more information on application definitions and application policies, see application and application-policy.</td>
</tr>
</tbody>
</table>

- **use captive-portal <CAPTIVE-PORTAL-NAME>**

  A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional terms and agreement, welcome, fail, and no-service pages provide the administrator with a number of options on captive portal screen flow and user appearance.

  - `<CAPTIVE-PORTAL-NAME>` – Specify the captive portal name.

- **use [ip-access-list|ipv6-access-list|mac-access-list] tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME>**

<table>
<thead>
<tr>
<th><strong>use</strong></th>
<th>Sets this VLAN bridge policy to use an IPv4/IPv6 access list or a MAC access list</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-access-list</strong></td>
<td>Associates a pre-configured IPv4 access list with this VLAN-bridge interface</td>
</tr>
<tr>
<td><strong>ipv6-access-list</strong></td>
<td>Associates a pre-configured IPv6 access list with this VLAN-bridge interface</td>
</tr>
</tbody>
</table>
### Mac-access-list

Associates a pre-configured MAC access list with this VLAN bridge interface.

### Tunnel out

**<IP/IPv6/MAC-ACCESS-LIST-NAME>**

The following keywords are common to the 'IPv4/IPv6 access list' and 'MAC access list' parameters:
- **tunnel** – Applies IPv4/IPv6 access list or MAC access list to all packets going into the tunnel
- **out** – Applies IPv4/IPv6 access list or MAC access list to all outgoing packets
- **<IP/IPv6/MAC-ACCESS-LIST-NAME>** – Specify the IP/IPv6 access list or MAC access list name.

#### Examples

```bash
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#use mac-access-list tunnel out PERMIT-ARP-AND-IPv4
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
  bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
use mac-access-list tunnel out PERMIT-ARP-AND-IPv4
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

### Related Commands

- **no**
  
  Disables or reverts VLAN Ethernet bridge settings.
7.1.12 captive-portal

Profile Config Commands

Configures captive portal advanced Web page uploads on this profile. These Web pages are uploaded to access points supporting the captive portal.

A captive portal is a means of providing guests temporary and restrictive access to the controller managed wireless network. A captive portal provides secure authenticated controller access by capturing and re-directing a wireless user’s Web browser session to a captive portal login page, where the user must enter valid credentials. Once the user is authenticated and logged into the controller managed network, additional agreement, welcome, and fail pages provide the administrator with options to control the captive portal’s screen flow and user appearance.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
captive-portal page-upload count <1-20>
```

Parameters

- **captive-portal page-upload count <1-20>**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>page-upload</td>
<td>Enables captive portal advanced Web page upload</td>
</tr>
<tr>
<td>count &lt;1-20&gt;</td>
<td>Sets the maximum number of APs that can be uploaded concurrently</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-20&gt; – Set a value from 1 - 20. The default is 10.</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-profile-default-rfs7000)#captive-portal page-upload count 10
rfs7000-37FABE(config-profile-default-rfs7000)#
```
### 7.1.13 cdp

#### Profile Config Commands

Enables Cisco Discovery Protocol (CDP), a proprietary data link layer network protocol implemented in Cisco networking equipment and used to share network information amongst different vendor wireless devices.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```
cdp [holdtime|run|timer]
cdp [holdtime <10-1800>|run|timer <5-900>]
```

### Parameters

- `cdp [holdtime <10-1800>|run|timer <5-900>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>holdtime &lt;10-1800&gt;</code></td>
<td>Specifies the holdtime after which transmitted packets are discarded</td>
</tr>
<tr>
<td><code>run</code></td>
<td>Enables CDP sniffing and transmit globally. This feature is enabled by default.</td>
</tr>
<tr>
<td><code>timer &lt;5-900&gt;</code></td>
<td>Specifies the interval, in seconds, between successive CDP packet transmission</td>
</tr>
</tbody>
</table>

### Examples

```
rfs7000-37FABE(config profile-default-rfs7000)#cdp run
rfs7000-37FABE(config profile-default-rfs7000)#cdp holdtime 1000
rfs7000-37FABE(config profile-default-rfs7000)#cdp timer 900
rfs7000-37FABE(config-profile-default-rfs7000)#show context
```

### Related Commands

- `no` Disables CDP on this profile
7.1.14 cluster

Profile Config Commands

Sets the cluster configuration

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

cluster [force-configured-state|force-configured-state-delay <3-1800>|handle-stp|master-priority <1-255>]

cluster member [ip|vlan]

cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]

cluster mode [active|standby]

cluster name <CLUSTER-NAME>

cluster radius-counter-db-sync-time <1-1440>

Parameters

- force-configured-state
  - Forces adopted APs to auto revert when a failed wireless controller or service platform (in a cluster) restarts
  - When an active controller (wireless controller, or service platform) fails, a standby controller in the cluster takes over APs adopted by the failed active controller. If the failed active controller were to restart, it starts a timer based on the ‘force-configured-state-delay’ interval specified. At the expiration of this interval, the standby controller releases all adopted APs and goes back to a monitoring mode. If the active controller fails during this interval, the ‘force-configured-state-delay’ timer is stopped. The timer restarts as soon as the active controller comes back up.
  - This feature is disabled by default.

- force-configured-state-delay <3-1800>
  - Forces cluster transition to the configured state after a specified interval
  - <3-1800> – Specify a delay from 3 - 1800 minutes. The default is 5 minutes.
  - This is the interval a standby controller waits before releasing adopted APs when a failed primary controller becomes active again.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>handle-stp</td>
<td>Enables Spanning Tree Protocol (STP) convergence handling. This feature is disabled by default. In layer 2 networks, this protocol is enabled to prevent network looping. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup.</td>
</tr>
</tbody>
</table>
| master-priority <1-255> | Configures cluster master priority  
  • <1-255> – Specifies cluster master election priority. Assign a value from 1 - 255. Higher the value higher is the precedence. The default is 128.  
  In a cluster environment one device from the cluster is elected as the cluster master. A device’s master priority value decides the device’s priority to become cluster master. |
| member                  | Adds a member to the cluster. It also configures the cluster VLAN where members can be reached.                                                                                                             |
| ip <IP> level [1|2]    | Adds IP address of the new cluster member  
  • <IP> – Specify the IP address.  
  • level – Optional. Configures routing level for the new member. Select one of the following routing levels:  
    • 1 – Level 1, local routing  
    • 2 – Level 2, In-site routing |
| vlan <1-4094>           | Configures the cluster VLAN where members can be reached  
  • <1-4094> – Specify the VLAN ID from 1- 4094. |
| mode [active|standby]         | Configures cluster member’s mode as active or standby  
  • active – Configures cluster mode as active. This is the default setting.  
  • standby – Configures cluster mode as standby  
  A member can be in either an Active or Standby mode. All active member controllers can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller. |
| name <CLUSTER-NAME>     | Configures the cluster name  
  • <CLUSTER-NAME> – Specify the cluster name. |
| radius-counter-db-sync-time <1-1440> | Configures the interval, in minutes, at which the RADIUS counter database is synchronized with the dedicated NTP server resource.  
  • <1-1440> – Specify a value from 1 - 1440 minutes. The default is 5 minutes.  
  **Note:** Use the `show > cluster > configuration` command to view RADIUS counter DB sync time. |

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#cluster name cluster1
rfs7000-37FABE(config-profile-default-rfs7000)#cluster member ip 172.16.10.3
```
rfs7000-37FABE(config-profile-default-rfs7000)#cluster mode active

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
    description Vlan1

rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes cluster member</td>
</tr>
</tbody>
</table>
7.1.15 configuration-persistence

Profile Config Commands

Enables configuration persistence across reloads. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
configuration-persistence {auto|secure}

Parameters
- configuration-persistence {auto|secure}

Examples
rfs7000-37FABE(config-profile-default-rfs7000)#configuration-persistence secure
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  no edge-vlan
  ip igmp snooping
  no ip igmp snooping unknown-multicast-fwd
  no ip igmp snooping mrouter learn pim-dvmrp
  autoinstall configuration
  autoinstall firmware
  .................................................................
  cluster name cluster1
  cluster member ip 1.2.3.4 level 2
  cluster member ip 172.16.10.3
  cluster member vlan 4694
  cluster handle-stp
  cluster force-configured-state
  holdtime 1000
  timer 900
  configuration-persistence secure
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

- no Disables automatic write up of startup configuration file
7.1.16 controller

Profile Config Commands

- Configures the WiNG controller (wireless controller or service platform) adoption settings
- Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the adopted device. Adoption settings are configurable and supported within a profile and applied to all devices supported by the profile.
- Use this command to add a controller to a pool and group. This command also enables and disables adoption on controllers, and specifies the device types that can be adopted by a controller.
- In an hierarchically managed (HM) network, devices (controllers and access points) are deployed across three levels. This results in devices that are either adoptee or adopters. For more information on HM network, see device-upgrade.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

controller [adopted-devices|adoption|group|hello-interval|vlan|host]
controller adopted-devices [aps {controllers}|controllers {aps}|external-devices|external-devices-monitoring-only]
controller adoption
controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]
controller hello-interval <1-120> adjacency-hold-time <2-600>
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure|level|pool|remote-vpn-client}
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}{level [1/2]|pool <1-2> level [1/2]}
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {remote-vpn-client}

Parameters

- controller adopted-devices [aps {controllers}|controllers {aps}|external-devices|external-devices-monitoring-only]
  - adopted-devices
    - Configures the types of device (AP/controller) this controller can adopt
  - aps {controllers}
    - Enables the adoption of network access points by this controller. This option is enabled by default.
      - controllers – Optional. Enables the adoption of peer controllers by this controller
      - All adopted devices (referred to as adoptee) receive complete configuration from the adopting controller (referred to as adopter).
  - controllers {aps}
    - Enables the adoption of peer controllers by this controllers
      - aps – Optional. Enables the adoption of network access points by this controller
      - A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted controller (adoptee) cannot be configured to adopt another controller.
      - Use the no > controller > adopted-devices command to remove this setting.
### external-devices
Enables adoption of external devices by this controller. This option is disabled by default.

When enabled, a WiNG controller can adopt and manage T5 controllers and EX3500 switches (using the IPX operating system) within a WiNG managed device subnet. This setting is disabled by default.

To disable T5 or EX3500 adoption, use the `no > controller > external-devices` command.

**Note:** This feature is supported only on RFS4000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, and NX9600 platforms.

### external-devices-monitoring-only
Enables only monitoring of external devices by this controller or service platform. This option is disabled by default.

### • controller adoption

**controller adoption**
Enables the adoption of the logged device (wireless controller or service platform) by other controllers. This option is disabled by default.

Use the `no > controller > adoption` command to disable adoption.

### • controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]

<table>
<thead>
<tr>
<th>controller</th>
<th>Configures the WLAN’s controller adoption settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Configures the wireless controller or service platform group</td>
</tr>
<tr>
<td>&lt;CONTROLLER-GROUP-NAME&gt;</td>
<td>• &lt;CONTROLLER-GROUP-NAME&gt; – Specify the wireless controller or service platform group name.</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Configures the wireless controller or service platform VLAN</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094.</td>
</tr>
</tbody>
</table>

### • controller hello-interval <1-120> adjacency-hold-time <2-600>

<table>
<thead>
<tr>
<th>controller</th>
<th>Configures the WLAN’s controller settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello-interval &lt;1-120&gt;</td>
<td>Configures the hello-interval in seconds. This is the interval between consecutive hello packets exchanged between AP and wireless controller or service platform.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-120&gt; – Specify a value from 1 - 120 seconds.</td>
</tr>
<tr>
<td>adjacency-hold-time &lt;2-600&gt;</td>
<td>Configures the adjacency hold time in seconds. This is the time since the last received hello packet, after which the adjacency between wireless controller or service platform and AP is lost, and the link is re-established.</td>
</tr>
<tr>
<td></td>
<td>• &lt;2-600&gt; – Specify a value from 2 - 600 seconds.</td>
</tr>
</tbody>
</table>

### • controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}]

<table>
<thead>
<tr>
<th>controller</th>
<th>Configures the WLAN’s controller adoption settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>host [&lt;IPv4&gt;</td>
<td>&lt;IPv6&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;IPv4&gt; – Configures wireless controller or service platform’s IPv4 address</td>
</tr>
<tr>
<td></td>
<td>• &lt;IPv6&gt; – Configures wireless controller or service platform’s IPv6 address</td>
</tr>
<tr>
<td></td>
<td>• &lt;HOSTNAME&gt; – Configures wireless controller or service platform’s hostname</td>
</tr>
</tbody>
</table>
### ipsec-secure

```
{gw [<IP>|<HOSTNAME>]}  
```

| controller host [<IPv4>|<IPv6>|<HOSTNAME>] | Configures wireless controller or service platform’s IPv4/IPv6 address or name |
|--------------------------------------------|--------------------------------------------------------------------------|
| • <IPv4> – Configures wireless controller or service platform’s IPv4 address |
| • <IPv6> – Configures wireless controller or service platform’s IPv6 address |
| • <HOSTNAME> – Configures wireless controller or service platform’s name |

| level [1|2] | The following keywords are common to the ‘IP’, ‘IPv6’, and ‘hostname’ parameters: |
|----------|--------------------------------------------------------------------------------|
| • 1 – Optional. Level 1, local routing |
| • 2 – Optional. Level 2, inter-site routing |

| pool <1-2> level [1|2] | The following keywords are common to the ‘IP’, ‘IPv6’, and ‘hostname’ parameters: |
|-------------------------|--------------------------------------------------------------------------------|
| • <1-2> – Select either 1 or 2 as the pool. The default is 1. After selecting the pool, optionally select one of the following two routing levels: |
| • 1 – Optional. Level 1, local routing |
| • 2 – Optional. Level 2, inter-site routing |

| {ipsec-secure
{gw [<IP>|<HOSTNAME>]}|remote-vpn-client} | After specifying the routing level and or device’s pool, you can optionally specify the following: |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• ipsec-secure – Optional. Enables Internet Protocol Security (IPSec) peer authentication on the connection (link) between the adopting devices. This option is disabled by default.</td>
<td></td>
</tr>
<tr>
<td>• gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform</td>
<td></td>
</tr>
<tr>
<td>• &lt;IP&gt; – Use this option to specify the IPSec gateway’s IP address.</td>
<td></td>
</tr>
<tr>
<td>• &lt;HOSTNAME&gt; – Use this option to specify the IPSec gateway’s hostname.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If the gateway’s IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway.

<table>
<thead>
<tr>
<th>remote-vpn-client</th>
<th>Forces MiNT link creation protocol (MLCP) to use remote VPN connection on the controller</th>
</tr>
</thead>
</table>

The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none.

**Note:** When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route etc. are installed on the AP.
| controller host [<IPv4>|<IPv6>|<HOSTNAME>] | Configures the WLAN's controller settings |
|-------------------------------------------------|-------------------------------------------|
| host [<IPv4>|<IPv6>|<HOSTNAME>] | Configures wireless controller or service platform's IPv4/IPv6 address or hostname |
| • <IPv4> – Configures wireless controller or service platform's IPv4 address |
| • <IPv6> – Configures wireless controller or service platform's IPv6 address |
| • <HOSTNAME> – Configures wireless controller or service platform's name |
| remote-vpn-client | Forces MLCP to use remote VPN connection on the controller |
| | The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none. When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route etc. are installed on the AP. |

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000)#controller group test
rfs7000-37FABE(config-profile-default-rfs7000)#controller host 1.2.3.4 pool 2
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
no autoinstall configuration
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface ge1
   ip dhcp trust
   qos trust dscp
   qos trust 802.1p
interface ge4
   ip dhcp trust
   qos trust dscp
   qos trust 802.1p
use firewall-policy default
ccontroller host 1.2.3.4 pool 2
ccontroller group test
service pm sys-restart
rfs4000-229D58(config-profile-testRFS4000)#controller adopted-devices aps controllers
rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
autoinstall configuration
logging on
service pm sys-restart
router ospf
ccontroller adopted-devices aps controllers
rfs4000-229D58(config-profile-testRFS4000)#

**Related Commands**

| no | Disables or reverts settings to their default |
7.1.17 critical-resource

Profile Config Commands

Enables monitoring of resources critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses. When enabled, the system monitors these devices regularly and logs their status. Use this command to create a critical resource monitoring (CRM) policy.

A critical resource can be a gateway, AAA server, WAN interface, any hardware, or a service on which the stability of the network depends. Monitoring these resources is therefore essential. When enabled, this feature pings critical resources regularly to ascertain their status. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there is no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as an AP8132 access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

Critical resource monitoring can be enabled on service platforms, wireless controllers, and access points through their respective device profiles.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

critical-resource [<CRM-POLICY-NAME>|monitor]
critical-resource <CRM-POLICY-NAME> [monitor|monitor-using-flows]
critical-resource <CRM-POLICY-NAME> monitor [direct|via]
critical-resource <CRM-POLICY-NAME> monitor direct [all|any] [<IP>|sync-adoptees] {<IP>|arp-only vlan <1-4094> {<IP>|port [<LAYER2-IF-NAME]|ge <1-4>|port-channel <1-2>}}
critical-resource <CRM-POLICY-NAME> monitor via [<IP]>[<LAYER3-INTERFACE-NAME]> pppoe1|vlan|wwan1

critical-resource <CRM-POLICY-NAME> monitor via [<IP]>[<LAYER3-INTERFACE-NAME>] pppoe1|vlan <1-4094>|wwan1] [all|any] [<IP>|sync-adoptees] {<IP>|arp-only vlan <1-4094> {<IP>|port [<LAYER2-IF-NAME]|ge <1-4>|port-channel <1-2>}}
critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] [criteria|dhcp|dns] sync-adoptees

critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dhcp vlan <1-4094> {dhcp vlan <1-4094>|dns <IP/HOST-ALIAS-NAME>}
critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dns <IP/HOST-ALIAS-NAME> {dhcp vlan <1-4094>|dns <IP/HOST-ALIAS-NAME>}
critical-resource monitor interval <5-86400>
**Parameters**

- `critical-resource <CRM-POLICY-NAME> monitor direct [all|any] [<IP>|sync-adoptees] {<IP>|arp-only vlan <1-4094> {<IP>|port [<LAYER2-IF-NAME>|ge <1-4>|port-channel <1-2>]]}

- `critical-resource <CRM-POLICY-NAME> monitor via [<IP]|<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [all|any] [<IP>|sync-adoptees] {<IP>|arp-only [vlan <1-4094>] {<IP>|port [<LAYER2-IF-NAME>|ge|port-channel]}}

<table>
<thead>
<tr>
<th>&lt;CRM-POLICY-NAME&gt;</th>
<th>Creates a critical resource monitoring policy, identified by the &lt;CRM-POLICY-NAME&gt; keyword. Provide the CRM policy name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Enables critical resource(s) monitoring</td>
</tr>
</tbody>
</table>
| direct [all|any] [<IP>|sync-adoptees] | Monitors critical resources using the default routing engine  
  • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)  
  • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)  
  • <IP> – Configures the IP address of the critical resource being monitored (for example, the DHCP or DNS server). Specify the IP address in the A.B.C.D format.  
  • sync-adoptees – Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status. |
| arp-only vlan <1-4094> {<IP>|port [<LAYER2-IFNAME]|ge|port-channel]} | The following keywords are common to the ‘all’ and ‘any’ parameters:  
  • arp-only vlan <1-4094> – Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known.  
  • vlan <1-4094> – Specifies the VLAN ID on which to send the probing ARP requests. Specify the VLAN ID from 1 - 4094.  
  • <IP> – Optional. Limits ARP to a device specified by the <IP> parameter  
  • port [<LAYER2-IF-NAME>|ge|port-channel] – Optional. Limits ARP to a specified port |
| <CRM-POLICY-NAME> | Creates a critical resource monitoring policy, identified by the <CRM-POLICY-NAME> keyword. Provide the CRM policy name. |
| monitor | Enables critical resource(s) monitoring |
| via | Specifies the interface or next-hop via which the ICMP pings should be sent.  
  Configures the interface or next-hop via which ICMP pings are sent. This does not apply to IP addresses configured for arp-only. For interfaces which learn the default-gateway dynamically (like DHCP clients and PPP interfaces), use an interface name for VIA, or use an IP address. |
| <IP> | Specify the IP address of the next-hop via which the critical resource(s) are monitored. Configures up to four IP addresses for monitoring. All the four IP addresses constitute critical resources. |
| <LAYER3-INTERFACE-NAME> | Specify the layer 3 Interface name (router interface) |
### pppoe1
- Specifies PPP over Ethernet interface

### vlan <1-4094>
- Specifies the wireless controller or service platform’s VLAN interface. Specify VLAN ID from 1 - 4094.

### wwan1
- Specifies Wireless WAN interface

### [all|any] [<IP>|sync-adoptees]
- Monitors critical resources using the default routing engine
  - all – Monitors all resources that are going down (generates an event when all specified critical resource IP addresses are unreachable)
  - any – Monitors any resource that is going down (generates an event when any one of the specified critical resource IP address is unreachable)
  - <IP> – Configures the IP address of the critical resource being monitored (for example, the DHCP or DNS server). Specify the IP address in the A.B.C.D format.
  - sync-adoptees – Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status.

### arp-only
- The following keywords are common to the ‘all’ and ‘any’ parameters:
  - arp-only vlan <1-4094> – Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known.
  - vlan <1-4094> – Specifies the VLAN ID to send the probing ARP requests. Specify the VLAN ID from 1 - 4094.
  - <IP> – Optional. Limits ARP to a device specified by the <IP> parameter
  - port [<LAYER2-IF-NAME>|ge|port-channel] – Optional. Limits ARP to a specified port

### arp-only vlan <1-4094> {<IP>|
- port [<LAYER2-IF-NAME>|ge|port-channel]}

---

  - dhcp vlan <1-4094>|dns <IP/HOST-ALIAS-NAME>

### <CRM-POLICY-NAME>
- Creates a critical resource monitoring policy, identified by the <CRM-POLICY-NAME> keyword. Provide the CRM policy name.

### monitor-using-flows
- Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP discover, DHCP offer etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.

### [all|any]
- Configures how critical resource event messages are generated. Options include all and any.
  - all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)
  - any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)
| criteria [all|cluster-master] rf-domain-manager | Configures the resource that will monitor critical resources and update the rest of the devices in a group. Options include all, rf-domain-manager, or cluster-master.  
• all – Configures all devices within a group (cluster or RF Domain) as the monitoring resource  
• cluster-master – Configures the cluster master as the monitoring resource  
• rf-domain-manager – Configures the RF Domain manager as the monitoring resource |
|---|---|
| dhcp vlan <1-4094> | The following parameters are recursive and common to the ‘all’, ‘cluster-master’, and ‘rf-domain-manager’ keywords:  
• dhcp – Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.  
• vlan <1-4094> – Configures the VLAN on which the critical resource(s) is available  
  • <1-4094> – Specify the VLAN from 1 - 4094. |
| dns <IP/HOST-ALIAS-NAME> | The following parameters are recursive and common to the ‘all’, ‘cluster-master’, and ‘rf-domain-manager’ keywords:  
• dns – Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.  
• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |
| {dhcp vlan <1-4094>| dns <IP/HOST-ALIAS-NAME>} | The ‘dhcp’ and ‘dns’ parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).  
• dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.  
• vlan <1-4094> – Configures the VLAN on which the critical resource(s) is available  
  • <1-4094> – Specify the VLAN from 1 - 4094.  
• dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.  
• <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured). |

**critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dhcp vlan <1-4094> {dhcp vlan <1-4094>|dns <IP/HOST-ALIAS-NAME>}**

<table>
<thead>
<tr>
<th>&lt;CRM-POLICY-NAME&gt;</th>
<th>Creates a critical resource monitoring policy, identified by the &lt;CRM-POLICY-NAME&gt; keyword. Provide the CRM policy name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor-using-flows</td>
<td>Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.</td>
</tr>
<tr>
<td>CLI Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[all</td>
<td>any]</td>
</tr>
<tr>
<td></td>
<td>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</td>
</tr>
<tr>
<td></td>
<td>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</td>
</tr>
<tr>
<td>dhcp vlan &lt;1-4094&gt;</td>
<td>Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.</td>
</tr>
<tr>
<td></td>
<td>• vlan &lt;1-4094&gt; – Configures the VLAN on which the critical resource(s) is available</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the VLAN from 1 - 4094.</td>
</tr>
<tr>
<td>{dhcp vlan &lt;1-4094&gt;</td>
<td>dns &lt;IP/HOST-ALIAS-NAME&gt;}</td>
</tr>
<tr>
<td></td>
<td>• dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.</td>
</tr>
<tr>
<td></td>
<td>• vlan &lt;1-4094&gt; – Configures the VLAN on which the critical resource(s) is available</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the VLAN from 1 - 4094.</td>
</tr>
<tr>
<td></td>
<td>• dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP/HOST-ALIAS-NAME&gt; – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</td>
</tr>
</tbody>
</table>

- **critical-resource** <CRM-POLICY-NAME> monitor-using-flows [all|any]  
dns <IP/HOST-ALIAS-NAME> {dhcp vlan <1-4094>|dns <IP/HOST-ALIAS-NAME>}

<table>
<thead>
<tr>
<th>&lt;CRM-POLICY-NAME&gt;</th>
<th>Creates a critical resource monitoring policy, identified by the &lt;CRM-POLICY-NAME&gt; keyword. Provide the CRM policy name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor-using-flows</td>
<td>Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.</td>
</tr>
<tr>
<td>[all</td>
<td>any]</td>
</tr>
<tr>
<td></td>
<td>• all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</td>
</tr>
<tr>
<td></td>
<td>• any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</td>
</tr>
<tr>
<td>dns &lt;IP/HOST-ALIAS-NAME&gt;</td>
<td>Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP/HOST-ALIAS-NAME&gt; – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</td>
</tr>
</tbody>
</table>
The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names):

- **dhcp** – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.
  - vlan <1-4094> – Configures the VLAN on which the critical resource(s) is available
  - <1-4094> – Specify the VLAN from 1 - 4094.
- **dns** – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.
  - <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

### Table: Parameter Descriptions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**{dhcp vlan &lt;1-4094&gt;</td>
<td>dns &lt;IP/HOST-ALIAS-NAME&gt;}**</td>
</tr>
<tr>
<td>**critical-resource &lt;CRM-POLICY-NAME&gt; monitor-using-flows [all</td>
<td>any] sync-adoptees criteria [all</td>
</tr>
<tr>
<td><strong>monitor-using-flows</strong></td>
<td>Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.</td>
</tr>
<tr>
<td>**[all</td>
<td>any]**</td>
</tr>
<tr>
<td>- all</td>
<td>Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</td>
</tr>
<tr>
<td>- any</td>
<td>Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</td>
</tr>
<tr>
<td><strong>sync-adoptees</strong></td>
<td>Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status.</td>
</tr>
<tr>
<td>**criteria [all</td>
<td>cluster-master</td>
</tr>
<tr>
<td>- all</td>
<td>Configures all devices within a group (cluster or RF Domain) as the monitoring resource</td>
</tr>
<tr>
<td>- cluster-master</td>
<td>Configures the cluster master as the monitoring resource</td>
</tr>
<tr>
<td>- rf-domain-manager</td>
<td>Configures the RF Domain manager as the monitoring resource</td>
</tr>
<tr>
<td><strong>dhcp vlan &lt;1-4094&gt;</strong></td>
<td>The following parameters are recursive and common to the ‘all’, ‘cluster-master’, and ‘rf-domain-manager’ keywords:</td>
</tr>
<tr>
<td>- dhcp</td>
<td>Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.</td>
</tr>
<tr>
<td>- vlan &lt;1-4094&gt;</td>
<td>Configures the VLAN on which the critical resource(s) is available</td>
</tr>
</tbody>
</table>
| - <1-4094> | Specify the VLAN from 1 - 4094.
The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:

- **dns** – Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.
- `<IP/HOST-ALIAS-NAME>` – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

The ‘dhcp’ and ‘dns’ parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).

- **dhcp** – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.
- **vlan <1-4094>** – Configures the VLAN on which the critical resource(s) is available
  - `<1-4094>` – Specify the VLAN from 1 - 4094.
- **dns** – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.
- `<IP/HOST-ALIAS-NAME>` – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

### critical-resource monitor interval <5-86400>

- **monitor interval <5-86400>**
  - Configures the critical resource monitoring frequency
  - `<5-86400>` – Specifies the frequency in seconds. Specify the time from 5 - 86400 seconds. The default is 30 seconds.

### Examples
```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#critical-resource test monitor direct all 192.168.13.10 arp-only vlan 1
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#critical-resource monitor interval 40

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
rfs6000 B4-C7-99-6D-B5-D4
  use profile default-rfs6000
  use rf-domain default
  hostname rfs6000-6DB5D4
  license AP
  6c781f42a3638757d8849c382668b4ea4be8e483e2f986ae392eebcbde6a8f6f309443e93ad3123c3d76
  mint mlcp ip
  ip default-gateway 192.168.13.2
  interface vlan1
  ip address 192.168.13.16/24
  ip dhcp client request options all
  cluster mode standby
  cluster member ip 192.168.13.16 level 1
  controller host 192.168.13.13
  critical-resource monitor interval 40
  critical-resource test monitor direct all 192.168.13.10 arp-only vlan 1
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```
7.1.18 crypto

Profile Config Commands

Use the crypto command to define a system-level local ID for Internet Security Association and Key Management Protocol (ISAKMP) negotiation and to enter the ISAKMP policy, ISAKMP client, or ISAKMP peer command set. The following table summarizes crypto configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>Invokes commands used to configure ISAKMP policy, iSAKMP client, and ISAKMP peer</td>
<td>page 7-73</td>
</tr>
<tr>
<td>crypto-auto-ipsec-tunnel commands</td>
<td>Creates an auto IPSec VPN tunnel and enters its configuration mode</td>
<td>page 7-79</td>
</tr>
<tr>
<td>crypto-ikev1/ikev2-policy commands</td>
<td>Creates a crypto IKEv1/IKEv2 policy and enters its configuration mode</td>
<td>page 7-86</td>
</tr>
<tr>
<td>crypto-ikev1/ikev2-peer commands</td>
<td>Creates a IKEv1/IKEv2 peer and enters its configuration mode</td>
<td>page 7-94</td>
</tr>
<tr>
<td>crypto-map-config-commands</td>
<td>Creates a crypto map and enters its configuration mode</td>
<td>page 7-102</td>
</tr>
<tr>
<td>crypto-remote-vpn-client commands</td>
<td>Creates a remote VPN client and enters its configuration mode</td>
<td>page 7-127</td>
</tr>
</tbody>
</table>
7.1.18.1 crypto

Use the crypto command to define a system-level local ID for ISAKMP negotiation and enter the ISAKMP policy, ISAKMP client, or ISAKMP peer configuration mode.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable Security Association (SA) exists, it is used for transmission. Otherwise, IKE is used to establish a SA with the peer. If no SA exists (and the crypto map entry is “respond only”), the packet is discarded.

When a secured packet arrives on an interface, its Security Parameter Index (SPI) is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|ike-version|ikev1|ikev2|ipsec]
load-management|map|pki|plain-text-deny-acl-scope|remote-vpn-client]
crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]
crypto ike-version [ikev1-only|ikev2-only]
crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>
peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]
crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>
dpd-retries <1-100>|nat-keepalive <10-3600>peer <IKEV2-PEER>
policy <IKEV2-POLICY-NAME>|remote-vpn]
crypto ipsec [df-bit|security-association|transform-set]
crypto ipsec df-bit [clear|copy|set]
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|
seconds <120-86400>]
crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|
esp-aes-256|esp-des|esp-null] [esp-aes-xcbc-mac|esp-md5-hmac|esp-sha-hmac|
esp-sha256-hmac]
crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
crypto pki import crl <TRUSTPOINT-NAME> URL <1-168>
crypto plain-text-deny-acl-scope [global|interface]
crypto remote-vpn-client
```

Parameters

- crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-ipsec-secure</td>
<td>Configures the Auto IPSec Secure parameter settings. For Auto IPSec tunnel configuration commands, see crypto-auto-ipsec-tunnel commands.</td>
</tr>
<tr>
<td>enable-ike-uniques</td>
<td>Enables Internet Key Exchange (IKE) unique ID check For more information on IKE unique IDs, see remotegw.</td>
</tr>
<tr>
<td>load-management</td>
<td>Configures load management for platforms using software cryptography</td>
</tr>
</tbody>
</table>

- **crypto ike-version [ikev1-only|ikev2-only]**

| ike-version [ikev1-only|ikev2-only] | Selects and starts the IKE daemon |
|--------------------------------------|----------------------------------|
| ikev1-only – Enables support for IKEv1 tunnels only |
| ikev2-only – Enables support for IKEv2 tunnels only |

- **crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-1000>|nat-keepalive <10-3600>|peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]**

<table>
<thead>
<tr>
<th>ikev1</th>
<th>Configures the IKE version 1 parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>dpd-keepalive &lt;10-3600&gt;</td>
<td>Sets the global Dead Peer Detection (DPD) keep alive interval from 10 - 3600 seconds. This is the interval between successive IKE keep alive messages sent to detect if a peer is dead or alive. The default is 30 seconds.</td>
</tr>
<tr>
<td>dpd-retries &lt;1-1000&gt;</td>
<td>Sets the global DPD retries count from 1- 1000. This is the number of keep alive messages sent to a peer before the tunnel connection is declared as dead. The default is 5.</td>
</tr>
<tr>
<td>nat-keepalive &lt;10-3600&gt;</td>
<td>Sets the global NAT keep alive interval from 10 - 3600 seconds. This is the interval between successive NAT keep alive messages sent to detect if a peer is dead or alive. The default is 20 seconds.</td>
</tr>
<tr>
<td>peer &lt;IKEV1-PEER&gt;</td>
<td>Specify the name/Identifier for the IKEv1 peer. For IKEV1 peer configuration commands, see crypto-ikev1/ikev2-peer commands.</td>
</tr>
<tr>
<td>policy &lt;IKEV1-POLICY-NAME&gt;</td>
<td>Configures an ISKAMP policy. Specify the name of the policy. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations. For IKEV1 policy configuration commands, see crypto-ikev1/ikev2-policy commands.</td>
</tr>
<tr>
<td>remote-vpn</td>
<td>Specifies the IKEV1 remote-VPN server configuration (responder only)</td>
</tr>
</tbody>
</table>

- **crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|dpd-retries <1-1000>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|policy <IKEV2-POLICY-NAME>|remote-vpn]**

<table>
<thead>
<tr>
<th>ikev2</th>
<th>Configures the IKE version 2 parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>cookie-challenge-threshold &lt;1-100&gt;</td>
<td>Starts the cookie challenge mechanism after the number of half open IKE SAs exceeds the specified limit. Specify the limit from 1 - 100. The default is 5.</td>
</tr>
<tr>
<td>dpd-keepalive &lt;10-3600&gt;</td>
<td>Sets the global DPD keepalive interval from 10 - 3600 seconds. The default is 30 seconds.</td>
</tr>
<tr>
<td>dpd-retries &lt;1-100&gt;</td>
<td>Sets the global DPD retries count from 1 - 100. The default is 5.</td>
</tr>
<tr>
<td>nat-keepalive &lt;10-3600&gt;</td>
<td>Sets the global NAT keepalive interval from 10 - 3600 seconds. The default is 20 seconds.</td>
</tr>
<tr>
<td>peer &lt;IKEV2-PEER&gt;</td>
<td>Specify the name/Identifier for the IKEv2 peer</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| `crypto ipsec df-bit [clear|copy|set]` | Configures Don't-Fragment (DF) bit handling for encapsulating header. The options are:  
• clear – Clears the DF bit in the outer header and ignores in the inner header  
• copy – Copies the DF bit from the inner header to the outer header. This is the default setting.  
• set – Sets the DF bit in the outer header |
| `crypto ipsec security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]` | Configures the IPSec SAs lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds, which ever limit is reached first, ends the SA. When the SA lifetime ends it is renegotiated as a security measure.  
• kilobytes – Specifies a volume-based key duration (minimum is 500 KB and maximum is 2147483646 KB)  
• <500-2147483646> – Specify a value from 500 - 2147483646 KB. The default is 4608000 KB.  
• seconds – Specifies a time-based key duration (minimum is 120 seconds and maximum is 86400 seconds)  
• <120-86400> – Specify a value from 120 - 86400 seconds. The default is 3600 seconds.  
The security association lifetime can be overridden under crypto maps. |
| `crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|esp-aes-256|esp-des|esp-null] [esp-aes-xcbc-mac|esp-md5-hmac|esp-sha-hmac|esp-sha256-hmac]` | Defines the transform set configuration (authentication and encryption) for securing data. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic.  
• <TRANSFORM-SET-TAG> – Specify the transform set name.  
After specifying the transform set used by the IPSec transport connection, set the encryption method and the authentication scheme used with the transform set.  
The encryption methods available are: DES, 3DES, AES, AES-192 and AES-256.  
The authentication schemes available are: esp-md5-hmac and esp-sha-hmac. |

### Related Commands

- **remote-vpn**  
  Specifies an IKEv2 remote-VPN server configuration (responder only)
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>esp-aes</td>
<td>Configures the ESP transform using Advanced Encryption Standard (AES) cipher. The transform set is assigned to a crypto map using the map’s set &gt; transform-set command.</td>
</tr>
<tr>
<td>esp-aes-192</td>
<td>Configures the ESP transform using AES cipher (192 bits). The transform set is assigned to a crypto map using the map’s set &gt; transform-set command.</td>
</tr>
<tr>
<td>esp-aes-256</td>
<td>Configures the ESP transform using AES cipher (256 bits). The transform set is assigned to a crypto map using the map’s set &gt; transform-set command. This is the default setting.</td>
</tr>
<tr>
<td>esp-des</td>
<td>Configures the ESP transform using Data Encryption Standard (DES) cipher (56 bits). The transform set is assigned to a crypto map using the map’s set &gt; transform-set command.</td>
</tr>
<tr>
<td>esp-null</td>
<td>Configures the ESP transform with no encryption</td>
</tr>
<tr>
<td>[esp-aes-xcbc-mac</td>
<td>esp-md5-hmac</td>
</tr>
<tr>
<td></td>
<td>• esp-aes-xcbc-mac – Configures ESP transform using AES-XCBC authorization</td>
</tr>
<tr>
<td></td>
<td>• esp-md5-hmac – Configures ESP transform using HMAC-MD5 authorization</td>
</tr>
<tr>
<td></td>
<td>• esp-sha-hmac – Configures ESP transform using HMAC-SHA authorization. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• esp-sha256-hmac – Configures ESP transform using HMAC-SHA256 authorization</td>
</tr>
</tbody>
</table>

- crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]

- map <CRYPTO-MAP-TAG> Configures the crypto map, a software configuration entity that selects data flows that require security processing. The crypto map also defines the policy for these data flows.
  - <CRYPTO-MAP-TAG> – Specify a name for the crypto map. The name should not exceed 32 characters. For crypto map configuration commands, see crypto-map-ipsec-manual-instance.

- <1-1000> Defines the crypto map entry sequence. Each crypto map uses a list of entries, each entry having a specific sequence number. Specifying multiple sequence numbers within the same crypto map provides the flexibility to connect to multiple peers from the same interface. Specify a value from 1 - 1000.

- ipsec-isakmp {dynamic} Configures IPSEC w/ISAKMP.
  - dynamic – Optional. Configures dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration

- ipsec-manual Configures IPSEC w/manual keying. Remote configuration is not allowed for manual crypto map.

- crypto pki import crl <TRUSTPOINT-NAME> <URL> <1-168>

- pki Configures certificate parameters. The Public Key Infrastructure (PKI) protocol creates encrypted public keys using digital certificates from certificate authorities.

- import Imports a trustpoint related configuration
crl  
<TRUSTPOINT-NAME>  Imports a Certificate Revocation List (CRL). Imports a trustpoint including either a private key and server certificate or a certificate authority (CA) certificate or both. A CRL is a list of revoked certificates that are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.  
  • <TRUSTPOINT-NAME> – Specify the trustpoint name.

<URL>  Specify the CRL source address in the following format. Both IPv4 and IPv6 address formats are supported.  
ftp://<hostname|IPv4 or IPv6>[:port]/path/file  
ftps://<hostname|IPv4 or IPv6>[:port]/path/file  
ftp://<user>:<passwd>@<hostname|IPv4 or IPv6>[:port]/path/file  
sftp://<user>:<passwd>@<hostname|IPv4 or IPv6>[:port]/path/file  
http://<hostname|IPv4 or IPv6>[:port]/path/file  
cf:/path/file  
usb<n>:/path/file

<1-168>  Sets command replay duration from 1 - 168 hours. This is the interval (in hours) after which devices using this profile copy a CRL file from an external server and associate it with a trustpoint.

• crypto plain-text-deny-acl-scope [global|interface]

plain-text-deny-acl-scope  Configures plain-text-deny-acl-scope parameters

| global  | Applies the plain text deny ACL globally. This is the default setting. |
| interface  | Applies the plain text deny ACL to the interface only |

• crypto remote-vpn-client

remote-vpn-client  Configures remote VPN client settings. For more information, see crypto-remote-vpn-client commands.

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ipsec transform-set tpsec-tag1 esp-aes-256 esp-md5-hmac
rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 10 ipsec-isakmp dynamic rfs7000-37FABE(config-profile-default-rfs7000)#crypto plain-text-deny-acl-scope interface
rfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000  
  bridge vlan 1  
  tunnel-over-level2  
  ip igmp snooping  
  ip igmp snooping querier  
  no autoinstall configuration  
  no autoinstall firmware  
  device-upgrade persist-images  
  crypto ikev1 dpd-retries 1  
  crypto ikev1 policy ikev1-default  
  isakmp-proposal default encryption aes-256 group 2 hash sha  
  crypto ikev2 policy ikev2-default  
  isakmp-proposal default encryption aes-256 group 2 hash sha  
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac  
  crypto ipsec transform-set tpsec-tag1 esp-aes-256 esp-md5-hmac
crypto map map1 10 ipsec-isakmp dynamic
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto plain-text-deny-acl-scope interface
  interface radio1
  interface radio2
  interface up
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto ipsec transform-set tag1 esp-null esp-md5-hmac

rfs7000-37FABE(config-profile-default-rfs7000-transform-set-tag1)#?

Crypto Ipsec Configuration commands:
  mode  Encapsulation mode (transport/tunnel)
  no    Negate a command or set its defaults
  clrscr  Clears the display screen
  commit  Commit all changes made in this session
  end  End current mode and change to EXEC mode
  exit  End current mode and down to previous mode
  help  Description of the interactive help system
  revert  Revert changes
  service  Service Commands
  show  Show running system information
  write  Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-transform-set-tag1)#

Related Commands

| no | Disables or reverts settings to their default |
7.1.18.2 crypto-auto-ipsec-tunnel commands

`crypto`

Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration.

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated access points that are within a range of valid IP addresses. You can define which packets are sent within the tunnel, and how they are protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination or associated access point.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

The IKE protocol is a key management protocol used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto auto-ipsec-secure
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#?
```

Crypto Auto IPSEC Tunnel commands:
- `groupid` Local/Remote identity and Authentication credentials for Auto IPsec Secure IKE negotiation
- `ike-lifetime` Set lifetime for ISAKMP security association
- `ikev2` IKEv2 configuration commands
- `ip` Internet Protocol config commands
- `no` Negate a command or set its defaults
- `remotegw` Auto IPSec Secure Remote Peer IKE

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

The following table summarizes the crypto IPSec auto tunnel configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>groupid</code></td>
<td>Specifies the identity string used for IKE authentication</td>
<td>page 7-80</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Enables the controller or service platform to uniquely identify APs and the hosts present in the AP's subnet</td>
<td>page 7-81</td>
</tr>
<tr>
<td><code>ike-lifetime</code></td>
<td>Configures the IKE SA's key lifetime in seconds</td>
<td>page 7-82</td>
</tr>
<tr>
<td><code>ikev2</code></td>
<td>Enables the forced re-authentication of IKEv2 peer</td>
<td>page 7-83</td>
</tr>
<tr>
<td><code>remotegw</code></td>
<td>Defines the IKE version used for an auto IPSec tunnel using secure gateways</td>
<td>page 7-84</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Removes or reverts the crypto auto IPSec tunnel settings</td>
<td>page 7-85</td>
</tr>
</tbody>
</table>
7.1.18.2.1 groupid

crypto-auto-ipsec-tunnel commands

Specifies the identity string used for IKE authentication

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

groupid <WORD> [psk|rsa]
groupid <WORD> [psk [0 <WORD>|2 <WORD>]<WORD>] |rsa]

Parameters

- groupid <WORD> [psk [0 <WORD>|2 <WORD>]<WORD>] |rsa]

| <WORD> | Specify a string not exceeding 64 characters. This is the group identity used for IKE exchange for auto IPSec secure peers. After providing a group ID, specify the authentication method used to authenticate peers on the auto IPSec secure tunnel. The options are: psk and rsa.
| psk [0 <WORD>|2 <WORD>]<WORD> | Configures the pre-shared key (PSK) as the authentication type for secure peer authentication on the auto IPSec secure tunnel
  - 0 <WORD> — Configures a clear text key
  - 2 <WORD> — Configures an encrypted key
  - <WORD> — Specify a string value from 8 - 21 characters.
| rsa | Configures the Rivest-Shamir-Adleman (RSA) key.
  RSA is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing, as well as encryption. This is the default setting.

NOTE: Only one group ID is supported on the controller or service platform. All APs, controllers, and service platform must use the same group ID.

Examples

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#groupid
testgroup@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
  groupid testgroup@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
7.1.18.2.2 ip

**crypto-auto-ipsec-tunnel commands**

Enables the controller to uniquely identify APs and the hosts present in the AP’s subnet. This allows the controller to correctly identify the destination host and create a dynamic site-to-site VPN tunnel between the host and the private network behind the controller.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ip nat crypto`

**Parameters**

- `ip nat crypto`

<table>
<thead>
<tr>
<th>ip nat crypto</th>
<th>Enables unique identification of APs and the hosts present in each AP’s subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. Further, the same subnet exists behind these APs. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). The subnet behind APs A and B is also the same (100.1.1.0/24). In such a scenario the controller fails to uniquely identify the hosts present in either AP’s subnet. For more information, see <code>remotegw</code> and <code>crypto</code>.</td>
</tr>
</tbody>
</table>

**Examples**

`rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#ip nat crypto`

`rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context crypto auto-ipsec-secure remotegw ike-version ikev2 uniqueid ip nat crypto rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#`
7.1.18.2.3 ike-lifetime

crypto-auto-ipsec-tunnel commands

Configures the IKE SA's key lifetime in seconds

The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ike-lifetime <600-86400>

Parameters

- ike-lifetime <600-86400>

<table>
<thead>
<tr>
<th>ike-lifetime &lt;600-86400&gt;</th>
<th>Sets the IKE SA's key lifetime in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;600-86400&gt;</td>
<td>- Specify a value from 600 - 86400 seconds. The default is 8600 seconds.</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58 (config-profile-testRFS4000-crypto-auto-ipsec-secure)#ike-lifetime 800

rfs4000-229D58 (config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context crypto auto-ipsec-secure

ike-lifetime 800

rfs4000-229D58 (config-profile-testRFS4000-crypto-auto-ipsec-secure)#
7.18.2.4 ikev2

**crypto-auto-ipsec-tunnel commands**

Enables the forced IKEv2 peer re-authentication. This option is disabled by default.

In most IPSec tunnel configurations, the lifetime of IKE SAs between peers is limited. Once the IKE SA key expires it is renegotiated. In such a scenario, the IKEv2 tunnel peers may or may not re-authenticate themselves. When enabled, IKE tunnel peers have to re-authenticate each time the IKE SA is renegotiated.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ikev2 peer reauth

**Parameters**

- ikev2 peer reauth

| ikev2 peer reauth | Enables IKEv2 peer re-authentication. When enabled, IKE tunnel peers are forced to re-authenticate each time the IKE key is renegotiated. |

**Examples**

rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#ikev2 peer reauth
7.1.18.2.5 remotegw

- **crypto-auto-ipsec-tunnel commands**

Defines the IKE version used for auto IPSEC tunnel negotiation with the IPSec remote gateway other than the controller

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

**Parameters**

- remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}

<table>
<thead>
<tr>
<th>remotegw ike-version</th>
<th>Configures the IKE version used for initiating auto IPSec tunnel with secure gateways other than the controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>ikev1-aggr</td>
<td>Aggregation mode is used by the auto IPSec tunnel initiator to set up the connection</td>
</tr>
<tr>
<td>ikev1-main</td>
<td>Main mode is used by the auto IPSec tunnel initiator to establish the connection</td>
</tr>
<tr>
<td>ikev2</td>
<td>IKEv2 is the preferred method when wireless controller/AP only is used</td>
</tr>
<tr>
<td>uniqueid</td>
<td>This keyword is common to all of the above parameters.</td>
</tr>
<tr>
<td></td>
<td>• uniqueid – Optional. Enables the assigning of a unique ID to APs (using this profile)</td>
</tr>
<tr>
<td></td>
<td>behind a router by prefixing the MAC address to the group ID</td>
</tr>
<tr>
<td></td>
<td>Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). In such a scenario, the controller fails to establish an Auto IPSec VPN tunnel to either APs, because it is unable to uniquely identify them. After enabling unique ID assignment, enable IKE unique ID check. For more information, see crypto.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#remotegw
ike-version ikev2 uniqueid

rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
remotegw ike-version ikev2 uniqueid
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```
7.1.18.2.6 no

*crypto-auto-ipsec-tunnel commands*

Removes or resets this auto IPSec tunnel settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`no [groupid|ike-lifetime|ikev2 peer reauth|ip nat crypto]`

**Parameters**

- `no <PARAMETERS>`

  Removes or resets this auto IPSec tunnel’s settings based on the parameters passed

**Examples**

The following example shows the Auto IPSec VLAN bridge settings before the ‘no’ command is executed:

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show context
  crypto auto-ipsec-secure
groupid testpassword@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#no groupid
```

The following example shows the Auto IPSec VLAN bridge settings after the ‘no’ command is executed:

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show context
  crypto auto-ipsec-secure
  no ikev2 peer reauth
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#
```

```
x45000-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#no ikev2 peer reauth
```

```
x45000-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
  crypto auto-ipsec-secure
    no ikev2 peer reauth
    ike-lifetime 800
x45000-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#
```

```
x45000-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#no ike-lifetime
```

```
x45000-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
  crypto auto-ipsec-secure
    no ikev2 peer reauth
x45000-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#
```
7.1.18.3 crypto-ikev1/ikev2-policy commands

`crypto`

Defines crypto-IKEv1/IKEv2 commands in detail

IKE protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs and enables secure communications without time consuming manual pre-configuration.

Use the (config) instance to configure IKEv1/IKEv2 policy configuration commands.

To navigate to the IKEv1/IKEv2 policy config instance, use the following commands:

```bash
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 policy <IKEV1/IKEV2-POLICY-NAME>
```

```bash
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev1 policy ikev1-testpolicy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#?
```

**Crypto IKEv1 Policy Configuration commands:**

- `dpd-keepalive` Set Dead Peer Detection interval in seconds
- `dpd-retries` Set Dead Peer Detection retries count
- `isakmp-proposal` Configure ISAKMP Proposals
- `lifetime` Set lifetime for ISAKMP security association
- `mode` IKEv1 mode (main/aggressive)
- `no` Negate a command or set its defaults
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
```

```bash
rfs7000-37FABE(config-profile-test-ikev2-policy-ikev2-testpolicy)#?
```

**Crypto IKEv2 Policy Configuration commands:**

- `dpd-keepalive` Set Dead Peer Detection interval in seconds
- `isakmp-proposal` Configure ISAKMP Proposals
- `lifetime` Set lifetime for ISAKMP security association
- `no` Negate a command or set its defaults
- `sa-per-acl` Setup single SA for all rules in the ACL (ONLY APPLICABLE FOR SITE-TO-SITE VPN)
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```bash
rfs7000-37FABE(config-profile-test-ikev2-policy-ikev2-testpolicy)#
```

---

**NOTE:** IKEv2 being an improved version of the original IKEv1 design, is recommended in most deployments. IKEv2 provides enhanced cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.
The following table summarizes crypto IKEv1/iKEv2 configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dpd-keepalive</td>
<td>Sets DPD keep alive packet interval</td>
<td>page 7-88</td>
</tr>
<tr>
<td>dpd-retries</td>
<td>Sets the maximum number of attempts for sending DPD keep alive packets (applicable only to the IKEv1 policy)</td>
<td>page 7-89</td>
</tr>
<tr>
<td>isakmp-proposal</td>
<td>Configures ISAKMP proposals</td>
<td>page 7-90</td>
</tr>
<tr>
<td>lifetime</td>
<td>Specifies how long an IKE SA is valid before it expires</td>
<td>page 7-91</td>
</tr>
<tr>
<td>mode</td>
<td>Sets the mode of the tunnels (applicable only to the IKEv1 policy)</td>
<td>page 7-92</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts IKEv1/IKEv2 policy settings</td>
<td>page 7-93</td>
</tr>
</tbody>
</table>
7.1.18.3.1 dpd-keepalive

Sets the DPD keep-alive packet interval

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6662, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dpd-keepalive <10-3600>

Parameters

- dpd-keepalive <10-3600>

| <10-3600> | Specifies the interval, in seconds, between successive DPD keep alive packets. The IKE keep alive message is used to detect a dead peer on the remote end of the IPSec VPN tunnel. Specify the time from 10 - 3600 seconds. The default is 30 seconds. |

Examples

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
dpd-keepalive 11

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show context
crypto ikev1 policy testpolicy
dpd-keepalive 11
isakmp-proposal default encryption aes-256 group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
7.1.18.3.2 dpd-retries

- **crypto-ikev1/ikev2-policy commands**

Sets the maximum number of times DPD keep-alive packets are sent to a peer. Once this value is exceeded, without a response from the peer, the VPN tunnel connection is declared dead. This option is available only for the IKEv1 policy.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dpd-retries <1-100>

**Parameters**

- dpd-retries <1-100>

<table>
<thead>
<tr>
<th>&lt;1-100&gt;</th>
<th>Declares a peer dead after the specified number of retries. Specify a value from 1 - 100. The default is 5.</th>
</tr>
</thead>
</table>

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#dpd-retries 10

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show context crypto ikev1 policy testpolicy
dpd-keepalive 11
dpd-retries 10
isakmp-proposal default encryption aes-256 group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
7.1.18.3.3 isakmp-proposal

- crypto-ikev1/ikev2-policy commands

Configures ISAKMP proposals and their parameters

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```bash
isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5]
hash [aes-xcbc-mac|md5|sha|sha256]
```

Parameters

- ```<WORD>``` Assigns the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration.
- ```encryption [3des|aes|aes-192|aes-256]``` Configures the encryption method used by the tunneled peers to securely interoperate.
  - 3des – Configures triple data encryption standard
  - aes – Configures AES (128 bit keys)
  - aes-192 – Configures AES (192 bit keys)
  - aes-256 – Configures AES (256 bit keys). This is the default setting.
- ```group [14|2|5]``` Specifies the Diffie-Hellman (DH) group identifier used by VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include 2, 5 and 14.
  - 14 – Configures DH group 14
  - 2 – Configures DH group 2. This is the default setting.
  - 5 – Configures DH group 5
- ```hash [aes-xcbc-mac|md5|sha|sha256]``` Specifies the hash algorithm used to authenticate data transmitted over the IKE SA. The hash algorithm specified here is used by VPN peers to exchange credential information.
  - aes-xcbc-mac – Uses AES XCBC Auth hash algorithm. This option is applicable only to the IKEv2 policy configuration context.
  - md5 – Uses Message Digest 5 (MD5) hash algorithm
  - sha – Uses Secure Hash Authentication (SHA) hash algorithm. This is the default setting.
  - sha256 – Uses Secure Hash Standard 2 algorithm

Examples

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
isakmp-proposal testproposal encryption aes group 2 hash sha

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#show context
crypto ikev1 policy testpolicy
dpd-keepalive 11
dpd-retries 10
isakmp-proposal default encryption aes-256 group 2 hash sha
isakmp-proposal testproposal encryption aes group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
```
7.1.18.3.4 lifetime

**crypto-ikev1/ikev2-policy commands**

Specifies how long an IKE SA (encryption/authentication keys) is valid. The value specified is the validity period of the IKE SA from successful key negotiation to expiration.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

lifetime <600-86400>

**Parameters**
- lifetime <600-86400>

<table>
<thead>
<tr>
<th>lifetime &lt;600-86400&gt;</th>
<th>Specifies how many seconds an IKE SA lasts before it expires. Set a time stamp from 600 - 86400 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;600-86400&gt;</td>
<td>&lt;600-86400&gt; – Specify a value from 600 - 86400 seconds. The default is 86400 seconds.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-test-ikevpolicy)#lifetime 655
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show context crypto ikev1 policy testpolicy
dpd-keepalive 11
dpd-retries 10
lifetime 655
isakmp-proposal default encryption aes-256 group 2 hash sha
isakmp-proposal testproposa1 encryption aes group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```
7.1.18.3.5 mode

crypto-ikev1/ikev2-policy commands

Configures the IPSec mode of operation for the IKEv1 policy. This option is not available for IKEv2 policy.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

tmode [aggressive|main]

Parameters

- mode [aggressive|main]

| mode [aggressive|main] | Sets the mode of the tunnels |
|------------------------|------------------------------|
| aggressive             | Initiates the aggressive mode |
| main                   | Initiates the main mode |

Note: If configuring the IKEv1 IPSec policy, define the IKE mode as either main or aggressive. In the aggressive mode, 3 messages are exchanged between the IPSec peers to setup the SA. On the other hand, in the main mode, 6 messages are exchanged. The default setting is main.

Examples

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#mode aggressive
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show context crypto ikev1 policy testpolicy
dpd-keepalive 11
dpd-retries 10
lifetime 655
isakmp-proposal default encryption aes-256 group 2 hash sha
isakmp-proposal testproposal encryption aes group 2 hash sha
mode aggressive
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
7.1.18.3.6 no

- **crypto-ikev1/ikev2-policy commands**
  - Removes or reverts IKEv1/IKEv2 policy settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```
no [dpd-keepalive|dpd-retries|isakmp-proposal <WORD>|lifetime|mode]
```

### Parameters
- `no <PARAMETERS>`

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes or reverts this IKEv1/IKEv2 policy settings based on parameters passed</th>
</tr>
</thead>
</table>

### Examples

The following example shows the IKEV1 Policy settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show context crypto ikev1 policy testpolicy
dpd-keepalive 11
dpd-retries 10
lifetime 655
isakmp-proposal default encryption aes-256 group 2 hash sha
isakmp-proposal testproposa encryption aes group 2 hash sha
mode aggressive
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```

The following example shows the IKEV1 Policy settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#no mode
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#no dpd-keepalive
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#no dpd-retries
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#show context crypto ikev1 policy testpolicy
lifetime 655
isakmp-proposal default encryption aes-256 group 2 hash sha
isakmp-proposal testproposa encryption aes group 2 hash sha
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-testpolicy)#
```
7.1.18.4 crypto-ikev1/ikev2-peer commands

Use the (config) instance to configure IKEv1/IKEv2 peer configuration commands. To navigate to the IKEv1/IKEv2 peer config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 peer <IKEV1/IKEV2-PEER-NAME>
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev1 peer peer1
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#?
```

Crypto IKEV1 Peer Configuration commands:
- **authentication**: Configure Authentication credentials
- **ip**: Configure peer address/fqdn
- **localid**: Set local identity
- **no**: Negate a command or set its defaults
- **remoteid**: Configure remote peer identity
- **use**: Set setting to use
- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ikev2 peer peer1
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#?
```

Crypto IKEV2 Peer Configuration commands:
- **authentication**: Configure Authentication credentials
- **ip**: Configure peer address/fqdn
- **localid**: Set local identity
- **no**: Negate a command or set its defaults
- **remoteid**: Configure remote peer identity
- **use**: Set setting to use
- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **do**: Run commands from Exec mode
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

The following table summarizes crypto IPSec IKEv1/IKEv2 peer configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Configures a peer’s authentication mode and the pre-shared key</td>
<td>page 7-96</td>
</tr>
<tr>
<td>ip</td>
<td>Configures the peer’s IP address</td>
<td>page 7-97</td>
</tr>
<tr>
<td>localid</td>
<td>Configures a peer’s local identity details</td>
<td>page 7-98</td>
</tr>
<tr>
<td>remoteid</td>
<td>Configures a remote peer’s identity details</td>
<td>page 7-99</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>Associates an IKEv1 policy and IKEv2 policy with the IKEv1 and IKEv2 peer respectively</td>
<td>page 7-100</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Negates a command or reverts settings to their default. The no command, when used in the ISAKMP policy mode, defaults the ISAKMP protection suite settings.</td>
<td>page 7-101</td>
</tr>
</tbody>
</table>
7.1.18.4.1 authentication

crypto-ikev1/ikev2-peer commands

Configures IKEv1/IKEv2 peer’s authentication mode and the pre-shared key

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

authentication [psk|rsa]

authentication psk [0 <WORD>|2 <WORD>|<WORD>] {local|remote}

authentication rsa

Parameters

• authentication psk [0 <WORD>|2 <WORD>|<WORD>] {local|remote}

| psk [0 <WORD>|2 <WORD>|<WORD>] | Configures the authentication mode as pre-shared key (PSK). The PSK is a string, 8 - 12 characters long. It is shared by both ends of the VPN tunnel connection. If using IKEv2, both a local and remote string must be specified for handshake validation at both ends (local and remote) of the VPN connection.
| {local|remote} | Configures the pre-shared key
| 0 <WORD> | 0 <WORD> – Configures a clear text key
| 2 <WORD> | 2 <WORD> – Configures an encrypted key
| <WORD> | <WORD> – Configures the pre-shared key

The following keywords are available only in the IKEv2 peer configuration mode:

• local – Optional. Uses the specified key for local peer authentication only
• remote – Optional. Uses the specified key for remote peer authentication only

Note: In case the peer type is not specified, this string is used for authenticating both local and remote peers.

• authentication rsa

rsa

Configures the authentication mode as Rivest, Shamir, and Adleman (RSA). This is the default setting (for both IKEv1 and IKEv2).

RSA is the first known public-key cryptography algorithm designed signing and encryption. If configuring the IKEv2 peer, the ‘rsa’ option allows you to enable authentication at both ends of the VPN connection (local and remote).

Examples

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#authentication rsa

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#authentication psk 0 key@123456

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
  authentication psk 0 key@123456 local
  authentication psk 0 key@123456 remote

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
7.1.18.4.2 ip

**crypto-ikev1/ikev2-peer commands**

Sets the IP address or Fully Qualified Domain Name (FQDN) of the IPSec VPN peer used in the tunnel setup.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ip [address <IP>|fqdn <WORD>]
```

**Parameters**

- `address <IP>` Specify the peer device’s IP address.
- `fqdn <WORD>` Specify the peer device’s FQDN hostname.

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#ip address 172.16.10.12
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context crypto ikev1 peer peer1
   ip address 172.16.10.12
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#ip address 192.168.10.6
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context crypto ikev2 peer peer1
   ip address 192.168.10.6
   authentication psk 0 test@123456 local
   authentication psk 0 test@123456 remote
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```
7.1.18.4.3 localid

crypto-ikev1/ikev2-peer commands

Sets a IKEv1/IKEv2 peer’s local identity. This local identifier is used with this peer configuration for an IKE exchange with the target VPN IPSec peer.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

localid [address|autogen-uniqueid|dn|email|fqdn|string]

localid [address <IP>|autogen-uniqueid <WORD>|dn <WORD>|email <WORD>|fqdn <WORD>|

    string <WORD>]

Parameters

- localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]

<table>
<thead>
<tr>
<th>address &lt;IP&gt;</th>
<th>Configures the peer’s IP address. The IP address is used as local identity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>autogen-uniqueid &lt;WORD&gt;</td>
<td>Generates a localid using the device's unique identity. The system prefixes the device's unique identity to the string provided here. The device’s unique identity should be existing and configured. For more information on configuring a device’s unique identity, see autogen-uniqueid.</td>
</tr>
<tr>
<td>dn &lt;WORD&gt;</td>
<td>Configures the peer’s distinguished name. (for example, &quot;C=us ST=&lt;state&gt; L=&lt;location&gt; O=&lt;organization&gt; OU=&lt;org unit&gt;&quot;). The maximum length is 128 characters.</td>
</tr>
<tr>
<td>email &lt;WORD&gt;</td>
<td>Configures the peer’s e-mail address. The maximum length is 128 characters.</td>
</tr>
<tr>
<td>fqdn &lt;WORD&gt;</td>
<td>Configures the peer’s FQDN. The maximum length is 128 characters.</td>
</tr>
<tr>
<td>string &lt;WORD&gt;</td>
<td>Configures the peer’s identity string. The maximum length is 128 characters. This is the default setting.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#localid email bob@examplecompany.com

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context crypto ikev1 peer peer1
ip address 172.16.10.12
localid email bob@examplecompany.com
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
7.1.18.4.4 remoteid

crypto-ikev1/ikev2-peer commands

Configures a IKEv1/IKEV2 peer’s remote identity. This remote identifier is used with this peer configuration for an IKE exchange with the target VPN IPSec peer.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]

Parameters

- remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address &lt;IP&gt;</td>
<td>Configures the remote IKEv1/IKEV2 peer’s IP address. The IP address is used as the peer’s remote identity.</td>
</tr>
<tr>
<td>dn &lt;WORD&gt;</td>
<td>Configures the remote peer’s distinguished name. For example, “C=us ST=&lt;state&gt; L=&lt;location&gt; O=&lt;organization&gt; OU=&lt;org unit&gt;”. The maximum length is 128 characters.</td>
</tr>
<tr>
<td>email &lt;WORD&gt;</td>
<td>Configures the remote peer’s e-mail address. The maximum length is 128 characters.</td>
</tr>
<tr>
<td>fqdn &lt;WORD&gt;</td>
<td>Configures a peer’s FQDN. The maximum length is 128 characters.</td>
</tr>
<tr>
<td>string &lt;WORD&gt;</td>
<td>Configures a peer’s identity string. The maximum length is 128 characters.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#remoteid dn SanJose
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
  ip address 172.16.10.12
  remoteid dn SanJose
  localid email bob@examplecompany.com
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#remoteid address 157.235.209.63
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
  remoteid address 157.235.209.63
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
7.1.18.4.5 use

*crypto-ikev1/ikev2-peer commands*

Associates IKEv1/IKEv2 policy with the IKEv1/IKEv2 peer respectively

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

use ikev1-policy <IKEV1-POLICY-NAME>
use ikev2-policy <IKEV2-POLICY-NAME>

**Parameters**

- **use ikev1-policy <IKEV1-POLICY-NAME>**
  
  | use ikev1-policy <IKEV1-POLICY-NAME> | Specify the IKEv1 policy name. The local IKEv1 policy and the peer IKEv1 policy must have matching group settings for successful negotiations. |

- **use ikev2-policy <IKEV2-POLICY-NAME>**

  | use ikev2-policy <IKEV2-POLICY-NAME> | Specify the IKEv2 policy name. The local IKEv2 policy and the peer IKEv2 policy must have matching group settings for successful negotiations. |

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
ip address 172.16.10.12
remoteId dn SanJose
localid email bob@examplecompany.com
use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#use ikev2-policy test-ikev2policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
remoteId address 157.235.209.63
use ikev2-policy test-ikev2policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
7.1.18.4.6 no

- crypto-ikev1/ikev2-peer commands

Removes or reverts IKEv1/IKEv2 peer settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [authentication|ip|localid|remoteid|use <IKEv1/IKEv2-POLICY-NAME>]

Parameters

- no <PARAMETERS>

Examples

The following example shows the Crypto IKEV1 peer1 settings before the 'no' commands are executed:

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context crypto ikev1 peer peer1
   ip address 172.16.10.12
   remoteid dn SanJose
   localid email bob@examplecompany.com
   use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

The following example shows the Crypto IKEV1 peer1 settings after the 'no' commands are executed:

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#no localid
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#no remoteid
```

The following example shows the Crypto IKEV2 peer1 settings before the 'no' commands are executed:

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context crypto ikev2 peer peer1
   remoteid address 157.235.209.63
   use ikev2-policy test
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```

The following example shows the Crypto IKEV2 peer1 settings after the 'no' commands are executed:

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#no use ikev2-policy
```

The following example shows the Crypto IKEV2 peer1 settings after the 'no' commands are executed:

```bash
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context crypto ikev2 peer peer1
   remoteid address 157.235.209.63
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```
This section explains crypto map configuration mode commands in detail.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike. Each entry is given an index (used to sort the ordered list).

IPSec VPN provides a secure tunnel between two networked peers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

IKE is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

Use crypto maps to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include transform sets. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPSec peer, however for remote VPN deployments one crypto map is used for all the remote IPSec peers.

Use the (config) instance to enter the crypto map configuration mode. To navigate to the crypto-map configuration instance, use the following commands:

```
In the device-config mode:
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]

In the profile-config mode:
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
```

There are three different configurations defined for each listed crypto map: site-to-site manual (ipsec-manual), site-to-site-auto tunnel (ipsec-isakmp), and remote VPN client (ipsec-isakmp dynamic). With site-to-site deployments, an IPSec tunnel is deployed between two gateways, each at the edge of two different remote networks. With remote VPN, an access point located at remote branch defines a tunnel with a security gateway. This facilitates the end points in the branch office to communicate with the destination endpoints (behind the security gateway) in a secure manner.

Each crypto map entry is given an index (used to sort the ordered list).

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 1 ipsec-manual
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#?
```

Manual Crypto Map Configuration commands:

- **local-endpoint-ip**: Use this IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)
- **mode**: Set the tunnel mode
- **no**: Negate a command or set its defaults
- **peer**: Set peer
- **security-association**: Set security association parameters
- **session-key**: Set security session key parameters
- **use**: Set setting to use
- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **do**: Run commands from Exec mode
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal
The following table summarizes crypto map configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto-map auto-vpn-tunnel/remote-vpn-client instance</td>
<td>Configures an auto site-to-site VPN or remote VPN client</td>
<td>page 7-104</td>
</tr>
<tr>
<td>crypto-map ipsec-manual-instance</td>
<td>Configures a manual site-to-site VPN</td>
<td>page 7-118</td>
</tr>
</tbody>
</table>
7.18.5.1 crypto-map auto-vpn-tunnel/remote-vpn-client instance

**crypto-map-config-commands**

To navigate to the auto site-to-site VPN tunnel configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 1 ipsec-isakmp
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#?
```

**Site to Site Crypto Map Configuration commands:**

- `ip` : Internet Protocol config commands
- `local-endpoint-ip` : Use this IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)
- `no` : Negate a command or set its defaults
- `peer` : Add a remote peer
- `pfs` : Specify Perfect Forward Secrecy
- `security-association` : Security association parameters
- `transform-set` : Specify IPSec transform to use
- `use` : Set setting to use

```
clrscr : Clears the display screen
commit : Commit all changes made in this session
do : Run commands from Exec mode
end : End current mode and change to EXEC mode
exit : End current mode and down to previous mode
help : Description of the interactive help system
revert : Revert changes
service : Service Commands
show : Show running system information
write : Write running configuration to memory or terminal
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

To navigate to the remote VPN client configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp {dynamic}
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp {dynamic}
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 2 ipsec-isakmp dynamic
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#?
```

**Dynamic Crypto Map Configuration commands:**

- `local-endpoint-ip` : Use this IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)
- `modeconfig` : Set the mode config method
- `no` : Negate a command or set its defaults
- `peer` : Add a remote peer
- `pfs` : Specify Perfect Forward Secrecy
- `remote-type` : Set the remote VPN client type
- `security-association` : Security association parameters
- `transform-set` : Specify IPSec transform to use
- `use` : Set setting to use

```
clrscr : Clears the display screen
commit : Commit all changes made in this session
do : Run commands from Exec mode
end : End current mode and change to EXEC mode
exit : End current mode and down to previous mode
help : Description of the interactive help system
revert : Revert changes
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```
The following table lists the IPSec-Auto-VPN/Remote-VPN tunnel configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Enables this setting to utilize IP/Port NAT on the VPN tunnel.</td>
<td>page 7-106</td>
</tr>
<tr>
<td>local-endpoint-ip</td>
<td>Uses the configured IP as local tunnel endpoint address, instead of the</td>
<td>page 7-107</td>
</tr>
<tr>
<td></td>
<td>interface IP. This command is applicable to the site-to-site VPN tunnel and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remote VPN client.</td>
<td></td>
</tr>
<tr>
<td>modeconfig</td>
<td>Configures the mode config method (pull or push) associated with the</td>
<td>page 7-108</td>
</tr>
<tr>
<td></td>
<td>remote VPN client. This command is applicable only to the remote VPN client.</td>
<td></td>
</tr>
<tr>
<td>peer</td>
<td>Configures the IKEv1 or IKEv2 peer for the VPN tunnel.</td>
<td>page 7-109</td>
</tr>
<tr>
<td>pfs</td>
<td>Configures the <em>Perfect Forward Secrecy</em> (PFS) for the VPN tunnel.</td>
<td>page 7-110</td>
</tr>
<tr>
<td>remote-type</td>
<td>Configures the remote VPN client type as either None or XAuth.</td>
<td>page 7-111</td>
</tr>
<tr>
<td>security-association</td>
<td>Defines this automatic VPN tunnel’s IPSec SA settings.</td>
<td>page 7-112</td>
</tr>
<tr>
<td>transform-set</td>
<td>Applies a transform set (encryption and hash algorithms) to the VPN tunnel.</td>
<td>page 7-114</td>
</tr>
<tr>
<td></td>
<td>This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>Applies an existing and configured IP access list to the VPN tunnel.</td>
<td>page 7-115</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts site-to-site VPN tunnel or remote VPN client settings</td>
<td>page 7-116</td>
</tr>
</tbody>
</table>
7.18.5.2 ip

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Enables this setting to utilize IP/Port NAT on this auto site-to-site VPN tunnel. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
ip nat crypto

Parameters
- ip nat crypto

| ip nat crypto | Enables this setting to utilize IP/Port NAT on the site-to-site VPN tunnel. This setting is disabled by default. |

Examples

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
7.1.18.5.3 local-endpoint-ip

Uses the configured IP as local tunnel endpoint address, instead of the interface IP

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
local-endpoint-ip <IP>
```

**Parameters**

- `local-endpoint-ip <IP>`

| local-endpoint-ip | Configures the local VPN tunnel’s (site-to-site VPN tunnel or remote VPN client) endpoint IP address  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>• &lt;IP&gt; – Specify the IP address. The specified IP address must be available on the interface.</td>
</tr>
</tbody>
</table>

**Examples**

**Site-to-site VPN tunnel:**

```plaintext
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#local-endpoint-ip 192.168.13.10
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
  local-endpoint-ip 192.168.13.10
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

**Remote VPN client:**

```plaintext
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
  local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```
7.18.5.4 modeconfig

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Configures the mode config method (pull or push) associated with the remote VPN client.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
modeconfig [pull|push]

Parameters
- modeconfig [pull|push]

| modeconfig [pull|push] | Configures the mode config method associated with a remote VPN client. The options are: pull and push. The mode (pull or push) defines the method used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push. |

Examples
Remote VPN client:
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#modeconfig pull
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
  modeconfig pull
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)
7.1.18.5.5 peer

crypto-map auto-vpn-tunnel/remote-vpn-client instance

Configures the IKEV1 or IKEV2 peer for the auto site-to-site VPN tunnel or remote VPN client. The peer device can be specified either by its hostname or by its IP address. A maximum of three peers can be configured.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>

Parameters
- peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>

<table>
<thead>
<tr>
<th>peer &lt;1-3&gt;</th>
<th>Creates a new peer and configures the peer’s priority level. Peer ‘1’ is the primary peer, and peer ‘3’ is redundant.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ikev1 &lt;IKEV1-PEER-NAME&gt;</td>
<td>Configures an IKEV1 peer</td>
</tr>
<tr>
<td>• &lt;IKEV1-PEER-NAME&gt; – Specify the IKEV1 peer’s name.</td>
<td></td>
</tr>
<tr>
<td>ikev2 &lt;IKEV2-PEER-NAME&gt;</td>
<td>Configures an IKEV2 peer</td>
</tr>
<tr>
<td>• &lt;IKEV2-PEER-NAME&gt; – Specify the IKEV2 peer’s name.</td>
<td></td>
</tr>
</tbody>
</table>

Examples
Site-to-site tunnel:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#peer 1 ikev2 ikev2Peer1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context crypto map test 1 ipsec-isakmp
  peer 1 ikev2 ikev2Peer1
  local-endpoint-ip 192.168.13.10
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#peer 1 ikev1 RemoteIKEV1Peer1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context crypto map test 2 ipsec-isakmp dynamic
  peer 1 ikev1 RemoteIKEV1Peer1
  local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
7.1.18.5.6 pfs

```plaintext
• crypto-map auto-vpn-tunnel/remote-vpn-client instance
```

Configures Perfect Forward Secrecy (PFS) for the auto site-to-site VPN tunnel or remote VPN client. PFS is the key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include 2, 5 and 14. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
pfs [14|2|5]
```

**Parameters**

- `pfs [14|2|5]`

**Examples**

**Site-to-site VPN tunnel:**

```plaintext
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#pfs 5

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context crypto map test 1 ipsec-isakmp
   peer 1 ikev2 ikev2Peer1
   local-endpoint-ip 192.168.13.10
   pfs 5
   ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

**Remote VPN client:**

```plaintext
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#pfs 14

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context crypto map test 2 ipsec-isakmp dynamic
   peer 1 ikev1 RemoteIKEv1Peer1
   local-endpoint-ip 157.235.204.62
   pfs 14
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```
7.18.5.7 remote-type

`crypto-map auto-vpn-tunnel/remote-vpn-client instance`

Configures the remote VPN client type as either None or XAuth

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

remote-type [none|xauth]

**Parameters**

- remote-type [none|xauth]

**Examples**

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context crypto map test 2 ipsec-isakmp dynamic peer 1 ikev1 RemoteIKEv1Peer1 local-endpoint-ip 157.235.204.62 pfs 14 remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

**Note:** XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message.
7.18.5.8 security-association

`crypto-map auto-vpn-tunnel/remote-vpn-client instance`

Defines the IPSec SA's (created by this auto site-to-site VPN tunnel or remote VPN client) settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
security-association [inactivity-timeout|level|lifetime]
```

```
security-association [inactivity-timeout <120-86400>|level perhost]
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

Parameters

- `security-association [inactivity-timeout <120-86400>|level perhost]`
  - inactivity-timeout <120-86400>
    - Specifies an inactivity period, in seconds, for this IPSec VPN SA. Once the set value is exceeded, the association is timed out.
    - <120-86400> – Specify a value from 120 - 86400 seconds. The default is 900 seconds.
  - level perhost
    - Specifies the granularity level for this IPSec VPN SA
    - perhost – Sets the IPSec VPN SA's granularity to the host level

- `security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]`
  - lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
    - Defines the IPSec SA's lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association.
    - kilobytes <500-2147483646> – Defines volume based key duration. Specify a value from 500 - 2147483646 kilobytes. Select this option to define a connection volume lifetime (in kilobytes) for the duration of the IPSec VPN SA. Once the set volume is exceeded, the association is timed out. This option is disabled by default.
    - seconds <120-86400> – Defines time based key duration. Specify the time frame from 120 - 86400 seconds. Select this option to define a lifetime (in seconds) for the duration of the IPSec VPN SA. Once the set value is exceeded, the association is timed out. This option is disabled by default.

Examples

Site-to-site tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-association inactivity-timeout 200
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-association level perhost
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-association lifetime kilobytes 250000
```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
  security-association level perhost
   peer 1 ikev2 ikev2Peer1
   local-endpoint-ip 192.168.13.10
   pfs 5
   security-association lifetime kilobytes 250000
   security-association inactivity-timeout 200
   ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#security-association lifetime seconds 10000

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
   peer 1 ikev1 RemoteIKEv1Peer1
   local-endpoint-ip 157.235.204.62
   pfs 14
   security-association lifetime seconds 10000
   remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
7.1.18.5.9 transform-set

Applies a transform set (encryption and hash algorithms) to site-to-site VPN tunnel or remote VPN client. This command allows you to provide customized data protection for each crypto map can be customized with its own data protection and peer authentication schemes.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}
```

Parameters

- `transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}`

<table>
<thead>
<tr>
<th>transform-set &lt;TRANSFORM-SET-TAG&gt;</th>
<th>&lt;TRANSFORM-SET-TAG&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies a transform set. The transform set should be existing and configured.</td>
<td></td>
</tr>
<tr>
<td>- &lt;TRANSFORM-SET-TAG&gt; – Specify the transform set's name.</td>
<td></td>
</tr>
<tr>
<td>- &lt;TRANSFORM-SET-TAG&gt; – Optional. Specify a second transform set. You can provide multiple, space-separated, transform set tags.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

Site-to-site VPN tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#transform-set AutoVPN
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
  crypto map test 1 ipsec-isakmp
    security-association level perhost
    peer 1 ikev2 ikev2Peer1
    local-endpoint-ip 192.168.13.10
    pfs 5
    security-association lifetime kilobytes 250000
    security-association inactivity-timeout 200
  transform-set AutoVPN
  ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#transform-set RemoteVPN
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
  crypto map test 2 ipsec-isakmp dynamic
    peer 1 ikev1 RemoteIKEv1Peer1
    local-endpoint-ip 157.235.204.62
    pfs 14
    security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```
7.18.5.10 use

**crypto-map auto-vpn-tunnel/remote-vpn-client instance**

Applies an existing and configured IP access list to the auto site-to-site VPN tunnel or remote VPN client. Based on the IP access list’s settings traffic is permitted or denied across the VPN tunnel.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

**Parameters**
- `use ip-access-list <IP-ACCESS-LIST-NAME>`

<table>
<thead>
<tr>
<th>ip-access-list</th>
<th>Specify the IP access list name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP-ACCESS-LIST-NAME&gt;</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

**Site-to-site VPN tunnel:**

```sh
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)# use ip-access-list test
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)# show context
crypto map test 1 ipsec-isakmp
use ip-access-list test
security-association level perhost
    peer 1 ikev2 ikev2Peer1
    local-endpoint-ip 192.168.13.10
    pfs 5
    security-association lifetime kilobytes 250000
    security-association inactivity-timeout 200
    transform-set AutoVPN
    ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

**Remote VPN client:**

```sh
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)# use ip-access-list test1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)# show context
    crypto map test 2 ipsec-isakmp dynamic
    use ip-access-list test1
    peer 1 ikev1 RemoteIKEv1Peer1
    local-endpoint-ip 157.235.204.62
    pfs 14
    security-association lifetime seconds 10000
    transform-set RemoteVPN
    remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```
### 7.1.18.5.11 no

**crypto-map auto-vpn-tunnel/remote-vpn-client instance**

Removes or reverts the auto site-to-site VPN tunnel or remote VPN client settings

Supported in the following platforms:
- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [ip|local-endpoint-ip|modeconfig|peer|pfs|remote-type|security-association|
   transform-set|use]
```

**Parameters**

- `no <PARAMETERS>`

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes or resets this auto site-to-site/remote VPN settings based on the parameters passed</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the IPSec site-to-site VPN tunnel ‘test’ settings before the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
     use ip-access-list test
     security-association level perhost
     peer 1 ikev2 ikev2Peer1
     local-endpoint-ip 192.168.13.10
     pfs 5
     security-association lifetime kilobytes 250000
     security-association inactivity-timeout 200
     transform-set AutoVPN
     ip nat crypto
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no use ip-access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no security-association level perhost
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no pfs
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no local-endpoint-ip
```

The following example shows the IPSec site-to-site VPN tunnel ‘test’ settings after the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
     peer 1 ikev2 ikev2Peer1
     security-association lifetime kilobytes 250000
     security-association inactivity-timeout 200
     transform-set AutoVPN
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```
The following example shows the IPSec remote VPN client ‘test’ settings before the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
  use ip-access-list test2
  peer 1 ikev1 RemoteIKEv1Peer1
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  transform-set RemoteVPN
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

The following example shows the IPSec remote VPN client ‘test’ settings after the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no use ip-access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no peer 1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no transform-set
```

The following example shows the IPSec remote VPN client ‘test’ settings after the ‘no’ commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
  local-endpoint-ip 157.235.204.62
  pfs 14
  security-association lifetime seconds 10000
  remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```
7.18.5.12 crypto-map-ipsec-manual-instance

crypto-map-config-commands

To navigate to the automatic IPSec manual VPN tunnel configuration instance, use the following command:

In the device-config mode:

<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-manual

In the profile-config mode:

<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-manual

rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 3 ipsec-manual
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#?

Manual Crypto Map Configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-endpoint-ip</td>
<td>Use this IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)</td>
<td>page 7-119</td>
</tr>
<tr>
<td>mode</td>
<td>Sets the tunnel mode</td>
<td>page 7-120</td>
</tr>
<tr>
<td>peer</td>
<td>Sets the peer device’s IP address</td>
<td>page 7-121</td>
</tr>
<tr>
<td>security-association</td>
<td>Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by a crypto map</td>
<td>page 7-122</td>
</tr>
<tr>
<td>session-key</td>
<td>Defines encryption and authentication keys for a crypto map</td>
<td>page 7-123</td>
</tr>
<tr>
<td>use</td>
<td>Uses the configured IP access list</td>
<td>page 7-125</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts crypto map IPSec manual settings</td>
<td>page 7-126</td>
</tr>
</tbody>
</table>
7.1.18.5.13 local-endpoint-ip

- **crypto-map-ipsec-manual-instance**

Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
local-endpoint-ip <IP>
```

**Parameters**

- **local-endpoint-ip <IP>**

<table>
<thead>
<tr>
<th>local-endpoint-ip &lt;IP&gt;</th>
<th>Uses the configured IP as local tunnel’s endpoint address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;IP&gt; – Specify the IP address. The specified IP address must be available on the interface.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#local-endpoint-ip 172.16.10.3
```
7.1.18.5.14 mode

- **crypto-map-ipsec-manual-instance**

Sets the crypto map tunnel mode

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mode [transport|tunnel]
```

**Parameters**

- `mode [transport|tunnel]`

| mode [transport|tunnel] | Sets the mode of the tunnel for this crypto map |
|------------------------|-----------------------------------------------|
|                        | transport – Initiates transport mode          |
|                        | tunnel – Initiates tunnel mode (default setting) |

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#mode transport
```

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context crypto map map1 1 ipsec-manual
    mode transport
```

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
```
7.1.18.5.15 peer

Sets the peer device's IP address. This can be set for multiple remote peers. The remote peer can be an IP address.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
peer <IP>

Parameters
- peer <IP>

| peer <IP> | Enter the peer device's IP address. If not configured, it implies respond to any peer. |

Examples
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1)#peer 172.16.10.12

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1)#show context crypto map map1 ipsec-manual
peer 172.16.10.12

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1)#
7.1.18.5.16 security-association

crypto-map-ipsec-manual-instance

Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by this crypto map.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]

Parameters

- security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]

| lifetime [kilobytes <500-2147483646> | seconds <120-86400>] | Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association. |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| kilobytes <500-2147483646> | - Defines volume based key duration. Specify a value from 500 - 2147483646 bytes. |
| seconds <120-86400> | - Defines time based key duration. Specify the time frame from 120 - 86400 seconds. |

NOTE: This command is not applicable to the ipsec-manual crypto map.

Examples

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#security-association
lifetime seconds 123

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#show context
Command not applicable to this crypto map
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#
### 7.1.18.5.17 session-key

**crypto-map-ipsec-manual-instance**

Defines encryption and authentication keys for this crypto map

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7510, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-key [inbound</td>
<td>outbound] ah &lt;256-4294967295&gt; authenticator [md5</td>
</tr>
<tr>
<td>session-key [inbound</td>
<td>outbound] esp &lt;256-4294967295&gt; cipher [3des</td>
</tr>
</tbody>
</table>

#### Parameters

- **session-key [inbound|outbound] ah <256-4294967295> [0|2]authenticator [md5|sha]] <WORD>**
  - Configures authentication header (AH) as the security protocol for the security session.
  - **0** — Sets a clear text key
  - **2** — Sets an encrypted key
  - authenticator — Sets AH authenticator details
    - **md5** <WORD> — AH with MD5 authentication
    - **sha** <WORD> — AH with SHA authentication
  - <WORD> — Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x). AH-MD5: 32, AH-SHA: 40

- **session-key [inbound|outbound] esp <256-4294967295> [0|2]cipher [3des|aes|aes-192|aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>**
  - Configures Encapsulating Security Payloads (ESP) as the security protocol for the security session. This is the default setting.
  - **0** — Sets the SPI for the security association from 256 - 4294967295
  - The SPI (in combination with the destination IP address and security protocol) identifies the security association.
Examples

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#session-key inbound esp
273 cipher esp-null authenticator sha 58768979

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
    peer 172.16.10.2
    mode transport
        session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#

| [0|2|cipher | [3des|aes|aes-192|aes-256|des|esp-null]| |
|-----|---|---|---|---|---|---|---|
| • 0 – Sets a clear text key |
| • 2 – Sets an encrypted key |
| • cipher – Sets encryption/decryption key details |
| • 3des – ESP with 3DES encryption |
| • aes – ESP with AES encryption |
| • aes-192 – ESP with AES-192 encryption |
| • aes-256 – ESP with AES-256 encryption |
| • des – ESP with DES encryption |
| • esp-null – ESP with no encryption |
| • authenticator – Specify ESP authenticator details |
| • md5 <WORD> – ESP with MD5 authentication |
| • sha <WORD> – ESP with SHA authentication |
| • <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x): AH-MD5: 32, AH-SHA: 40 |
7.1.18.5.18 use

- crypto-map-ipsec-manual-instance

Associates an existing IP access list with this crypto map. The ACL protects the VPN traffic.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

use ip-access-list <IP-ACCESS-LIST-NAME>

**Parameters**

- use ip-access-list <IP-ACCESS-LIST-NAME>

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#use ip-access-list test

crypto-map map1 1 ipsec-manual
use ip-access-list test
peer 172.16.10.12
mode transport
session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
7.1.18.5.19 no

`crypto-map-ipsec-manual-instance`

Removes or resets this crypto map's settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [local-endpoint-ip|mode|peer|security-association|session-key|use]

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes or resets this crypto map settings based on the parameters passed |

Examples

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
  use ip-access-list test
  peer 172.16.10.12
  mode transport
  session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#no use ip-access-list
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#no peer
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#no mode

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
  session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#1)#
7.1.18.6 crypto-remote-vpn-client commands

This section documents the IKEV2 remote VPN client configuration settings. Use this command to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

Use the profile-config instance to configure remote VPN client settings. To navigate to the remote-vpn-client configuration instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto remote-vpn-client
<DEVICE>(config-profile-<PROFILE-NAME>-crypto-ikev2-remote-vpn-client)#
```

```
NOTE: To configure remote VPN client settings on a device, on the device’s configuration mode, use the `crypto > remote-vpn-client` command.
For example: rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto remote-vpn-client
```

```
NOTE: The following configuration enables a access point to adopt to a controller over the remote VPN link:
On a profile: rfs4000-229D58(config-profile-testRFS4000)#controller host <HOST-IP> remote-vpn-client
On a device: rfs4000-229D58(config-00-23-68-22-9D-58)#controller host <HOST-IP> remote-vpn-client
```

```
rfs4000-229D58(config)#profile rfs4000 testRFS4000
rfs4000-229D58(config-profile-testRFS4000)#
```

```
rfs4000-229D58(config-profile-testRFS4000)#crypto remote-vpn-client
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#?
```

Crypto IKEV2 Remote Vpn Client Config commands:
- `dhcp-peer` Configure parameters for peers received via DHCP option
- `no` Negate a command or set its defaults
- `peer` Add a remote peer
- `shutdown` Disable remote vpn client
- `transform-set` Specify IPSec transform to use
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and return to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

The following table summarizes crypto remote VPN client configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-peer</td>
<td>Configures DHCP peer’s local ID and authentication settings</td>
<td>page 7-128</td>
</tr>
<tr>
<td>peer</td>
<td>Adds a remote IKEV2 peer</td>
<td>page 7-129</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables the remote VPN client</td>
<td>page 7-130</td>
</tr>
<tr>
<td>transform-set</td>
<td>Associates an existing IPSec transform set with this remote VPN client</td>
<td>page 7-131</td>
</tr>
<tr>
<td>no</td>
<td>Removes the remote VPN client settings</td>
<td>page 7-132</td>
</tr>
</tbody>
</table>
7.1.18.6.1 dhcp-peer

* crypto-remote-vpn-client commands

Configures DHCP peer’s local ID and authentication settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-peer [authentication|localid]

dhcp-peer authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]

dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]

Parameters
- dhcp-peer authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
  - Configures the DHCP peer’s authentication type as PSK
    - 0 <WORD> – Configures a clear text authentication key
    - 2 <WORD> – Configures an encrypted authentication key
    - <WORD> – Provide a 8 - 21 character shared key password for DHCP peer authentication

- dhcp-peer authentication rsa
  - Configures the DHCP peer’s authentication type as RSA. This is the default setting.

- dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]
  - Configures the DHCP peer’s localid using one of the following options:
    - autogen-uniqueid - Generates a localid using the device's unique identity. The system prefixes the device's unique identity to the string provided here. The device's unique identity should be existing and configured. For more information on configuring a device's unique identity, see autogen-uniqueid.
    - <WORD> – Provide the string.
    - string - Uses the value provided here as the DHCP peer’s localid.
    - <WORD> - Provide the string.

Examples

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#dhcp-peer authentication psk 0 @123testing

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context crypto remote-vpn-client
dhcp-peer authentication psk 0 @123testing
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
7.1.18.6.2 peer

> **crypto-remote-vpn-client commands**

Configures IKEv2 peers and assigns them priorities for utilization with remote VPN client connections. A maximum of three (3) peers can be added to support redundancy.

IKEv2 uses an initial handshake in which VPN peers negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA. Additionally, a first IPSec SA is established during the initial SA creation. All IKEv2 messages are request/response pairs. It is the responsibility of the side sending the request to retransmit if it does not receive a timely response.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

**Parameters**

- **peer <1-3> ikev2 <IKEV2-PEER-NAME>**

<table>
<thead>
<tr>
<th>peer &lt;1-3&gt;</th>
<th>Adds a IKEv2 peer. You can add maximum of three (3) peers to achieve redundancy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3&gt;</td>
<td>Specify a priority level for the peer from 1 - 3 (1 = primary, 2 = secondary, and 3 = redundant).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ikev2</th>
<th>Specify the IKEv2 peer’s name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IKEV2-PEER-NAME&gt;</td>
<td>Note: The peer should be existing and configured. To configure an IKEv2 peer use the crypto &gt; ikev2 &gt; peer &gt; &lt;IKEV2-PEER-NAME&gt; command.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#peer 1 ikev2 ikev2Peer1
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#peer 2 ikev2 ikev2Peer2
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context crypto remote-vpn-client
peer 1 ikev2 ikev2Peer1
peer 2 ikev2 ikev2Peer2
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```
7.1.18.6.3 shutdown

crypto-remote-vpn-client commands

Disables remote-vpn-client on this profile or device. Remote VPN client feature is enabled by default.

To enable a disabled remote VPN client execute the no > shutdown command.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

shutdown

Parameters

None

Examples

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)# shutdown
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
7.1.18.6.4 transform-set

*crypto-remote-vpn-client commands*

Specifies the IPSec Transform set to use with this remote VPN client. A transform set is a combination of security protocols, algorithms, and other settings applied to IPSec protected client traffic.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
transform-set <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}
```

**Parameters**

- `transform-set <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}`

<table>
<thead>
<tr>
<th>transform-set</th>
<th>Associates an IPSec Transform (should be existing and configured) set with this remote VPN client. You can optionally associate more than one transform set with this remote VPN client configuration. List the transform set tags separated by a space.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>To configure a transform-set, use the <code>crypto &gt; ipsec &gt; transform-set</code> command in the profile or device configuration mode.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#transform-set TransformSet1

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context
crypto remote-vpn-client
peer 1 ikev2 ikev2Peer1
  transform-set TransformSet1
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```
7.1.18.6.5 no

**crypto-remote-vpn-client commands**

Removes the remote VPN client settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [dhcp-peer|peer <1-3>|shutdown|transform-set]

no dhcp-peer [authentication|localid]

no peer <1-3>

no shutdown

no transform-set

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Removes or resets this remote VPN client settings based on the parameters passed |

**Examples**

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context crypto remote-vpn-client

peer 1 ikev2 peer5

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#no peer 1

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context crypto remote-vpn-client

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
7.1.19 database-backup

Profile Config Commands

Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server. When applied to devices, this profile will enable the back up of the specified database.

Supported in the following platforms:

- Service Platforms — NX9000, NX9500, NX9510, NX9600

Syntax

database-backup database [captive-portal|nsight] <URL>

Parameters

- database-backup database [captive-portal|nsight] <URL>

| database-backup database [captive-portal|nsight] | Backs up captive portal and/or NSight database to a specified location and file. Select the database to backup
|<URL> | Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:

ftp://<user>:<passwd>@<hostname|IP>[;port]/path/file.tar.gz

sftp://<user>:<passwd>@<hostname|IP>[;port]/path/file.tar.gz

Examples

nx9500-6C8809(config-profile-testNX9000)#database-backup database nsight ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz

Related Commands

- no

Removes database backup configurations
7.1.20 device-upgrade

Profile Config Commands

Configures device firmware upgrade settings on this profile

Administrators can customize profiles with unique device configuration file and firmware upgrade support. In a clustered environment, operations performed on one device are propagated to each member of the cluster and then onwards to devices managed by each cluster member. The number of concurrent device upgrades and their start times can be customized to ensure a sufficient number of devices remain in duty while upgrades are administered to others.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

device-upgrade [add-auto|auto|count|persist-images]

device-upgrade add-auto [(ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600)]

device-upgrade auto {[(ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600)]}

device-upgrade count <1-128>

device-upgrade persist-images

Parameters
- device-upgrade add-auto
  Adds selected devices to the device type list. Specify the device type. The options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, NX9600.
  Note: Multiple device types can be added to the add-auto list.
  Note: The NX9600 option is available only on a NX9600 model service platform.
- **device-upgrade auto**: Enables automatic firmware upgrade on specified device types. When used along with the add-auto command, the auto command allows access points, wireless controllers, and service platforms to automatically upgrade firmware on adopted devices matching the specified device types.

  ```
  { (ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx75xx|nx9000|nx9600) }
  ```

  **Example**:
  ```
rfs4000-229D58(config-profile-default-rfs4000)#device-upgrade auto ap71xx
  ```

- **device-upgrade count <1-128>**: Configures the maximum number of concurrent upgrades possible. The default is 10.

  ```
  <1-128> – specify a value from 1 - 128. The default is 10.
  ```

- **device-upgrade persist-images**: Enables RF Domain manager to retain AP firmware image after upgrade, subject to availability of space. This option is enabled by default.

  ```
  This option is enabled for all controllers and service platforms RF Domain managers with the flash memory capacity to store firmware images for the selected access point models they provision. This feature is disabled for access point RF Domain managers that do not typically have the flash memory capacity needed.
  ```

- **Examples**:
  ```
rfs4000-229D58(config-profile-default-rfs4000)#device-upgrade auto ap71xx
  ```

- **Related Commands**:
  - `no`: Removes device firmware upgrade settings on this profile
  - `device-upgrade`: Displays device upgrade details
### 7.1.21 dot1x

#### Profile Config Commands

Configures 802.1x standard authentication controls.

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
  dot1x [guest-vlan|holdtime|system-auth-control|use]
```

- `dot1x holdtime <0-600>`
- `dot1x system-auth-control`
- `dot1x guest-vlan supplicant`
- `dot1x use aaa-policy <AAA-POLICY-NAME>`

**Parameters**

- `dot1x system-auth-control`

<table>
<thead>
<tr>
<th>system-auth-control</th>
<th>Enables system auth control. Enables dot1x authorization globally for the controller. This feature is disabled by default.</th>
</tr>
</thead>
</table>

- `dot1x holdtime <0-600>`

  | holdtime <0-600> | Configures a holdtime value. This is the interval after which an authentication attempt is ignored or failed.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-600&gt; – Specify a value from 0 - 600 seconds. A value of ‘0’ indicates no holdtime. The default is 600 seconds or 10 minutes. Adding a hold time at startup allows time for the network to converge before receiving or transmitting 802.1x authentication packets.</td>
<td></td>
</tr>
</tbody>
</table>

- `dot1x guest-vlan supplicant`

  | guest-vlan | Configures guest VLAN and supplicant behavior  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This feature is disabled by default.</td>
<td></td>
</tr>
</tbody>
</table>

  | supplicant | Allows 802.1x capable supplicant to enter guest VLAN. When enabled, this is the VLAN that supplicant's traffic is bridged on.  
  |------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
• dot1x use aaa-policy <AAA-POLICY-NAME>

<table>
<thead>
<tr>
<th>use aaa-policy &lt;AAA-POLICY-NAME&gt;</th>
<th>Associates a specified 802.1x AAA policy (for MAC authentication) with this access point profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;AAA-POLICY-NAME&gt; – Specify the AAA policy name. Once specified, this AAA policy is utilized for authenticating user requests.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

nx4500-5CFA2B(config-profile-testNX45XX)#dot1x use aaa-policy test

nx4500-5CFA2B(config-profile-testNX45XX)#dot1x system-auth-control

nx4500-5CFA2B(config-profile-testNX45XX)#show context profile nx45xx testNX45XX
  slot 1
  slot 2
  slot 3
  slot 4
  no autoinstall configuration
  no autoinstall firmware
  crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev1 peer peer1

  ..

  ipv6 nd raguard
  interface wwan1
  interface pppoe1
  use firewall-policy default
  service pm sys-restart
  router ospf
  router bgp
  dot1x system-auth-control
  dot1x use aaa-policy test
  service fast-switching

nx4500-5CFA2B(config-profile-testNX45XX)#

**Related Commands**

| no | Disables or reverts settings to their default |
7.1.22 dpi

Profile Config Commands

Enables Deep Packet Inspection (DPI) on this profile or device

DPI is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the WiNG managed network. DPI inspects every byte of each application header packet passing through the controller or service platform, and logs, blocks, or routes the packets to their destination. The level of granularity that DPI provides in terms of packet inspection helps block the spread of viruses, illegal downloads, and prioritizes data transmitted by bandwidth-heavy applications (video and VoIP applications), resulting in reduced congestion and enhanced security within the WiNG managed network.

This command is also available in the device configuration mode.

Supported in the following platforms:
• Access Points — AP7522, AP7532
• Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dpi {custom-app <CUSTOM-APP-NAME>|logging [level [<0-7> | alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]|on]}

Parameters

• dpi {custom-app <CUSTOM-APP-NAME>|logging [level [<0-7> | alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]|on]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dpi</td>
<td>Enables DPI (application assurance) on this profile and configures DPI settings When enabled, the system detects the Protocol and Application Classification Engine (PACE), a third-party DPI engine from IPOQUE, built-in applications. PACE has approximately 700 built-in applications that are grouped into twenty two (22) application categories. Use the 'custom-app' option to add applications not included in the PACE built-in list.</td>
</tr>
</tbody>
</table>
| custom-app| Optional. Adds custom application to this profile
|           | • <CUSTOM-APP-NAME> – Specify custom application name (should be existing and configured) If no custom application is specified, the system detects the PACE built-in applications. **Note:** For more information application categories and application detection, see application. |
| logging   | Optional. Enables DPI logging and sets the logging level level – Configures the DPI logging level. Use one of the following options to specify the logging level:
|           | • <0-7> Logging severity level
|           | • alerts Immediate action needed (1)
|           | • critical Critical conditions (2)
|           | • debugging Debugging messages (7)
|           | • emergencies System is unusable (0)
|           | • errors Conditions (3)
|           | • informational Informational messages (6)
|           | • notifications Normal but significant conditions (5) - Default setting
|           | • warnings Warning conditions (4)
|           | Either specify the logging level index (from 0 - 7) or the description. For example, to log all alerts either enter ‘1’ or ‘alerts’.
|           | • on – Enables application detection event logging. DPI logging is disabled by default. |
Examples

nx9500-6C8809(config-profile-testNX9000)#dpi logging on

nx9500-6C8809(config-profile-testNX9000)#dpi logging level 7

nx9500-6C8809(config-profile-testNX9000)#show context profile nx9000 testNX9000
  bridge vlan 10
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping

.........................................................

router bgp
  dpi logging on
  dpi logging level debugging

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables DPI (application assurance) on this profile</td>
</tr>
</tbody>
</table>
7.1.23 dscp-mapping

Profile Config Commands

Configures IP Differentiated Services Code Point (DSCP) to 802.1p priority mapping for untagged frames

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dscp-mapping <WORD> priority <0-7>

Parameters

- dscp-mapping <word> priority <0-7>

<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Specifies the DSCP value of a received IP packet. This could be a single value or a list. For example, 10-20, 25, 30-35.</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority &lt;0-7&gt;</td>
<td>Specifies the 802.1p priority to use for a packet if untagged. The priority is set on a scale of 0 - 7. The priority values are: 0 – Best effort, 1 – Background, 2 – Spare, 3 – Excellent effort, 4 – Controlled load, 5 – Video, 6 – Voice, 7 – Network control.</td>
</tr>
</tbody>
</table>

Note: The specified 802.1p priority value is added as a 3-bit IP precedence value in the Type of Service (ToS) field of the IP header used to set the priority. Up to 64 entries are permitted.

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#dscp-mapping 20 priority 7

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
dscp-mapping 20 priority 7
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface ge1
ip dhcp trust
qos trust dscp
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

- no | Disables or reverts settings to their default
### 7.1.24 email-notification

**Profile Config Commands**

Configures e-mail notification settings. When a system event occurs e-mail notifications are sent (provided message logging is enabled) based on the settings configured here. Use this option to configure the outgoing SMTP server settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
e-mail-notification [host|recipient]
e-mail-notification recipient <RECIPIENT-NAME>
e-mail-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL>
  [port|security|username]
e-mail-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL>
  [(port <1-65535>, security [none|ssl|starttls], username <SMTP-USERNAME> password [2 <WORD>|<WORD>])]
```

**Parameters**

- **recipient <RECIPIENT-EMAIL>**
  
  Defines the recipient’s e-mail address. A maximum of 6 (six) e-mail addresses can be configured.
  
  - `<RECIPIENT-EMAIL>` – Specify the recipient’s e-mail address (should not exceed 64 characters in length).

- **host <SMTP-SERVER-IP/HOSTNAME>**
  
  Configures the host SMTP server’s IP address or hostname.
  
  - `<SMTP-SERVER-IP/HOSTNAME>` – Specify the SMTP server’s IP address or hostname.

- **sender <SENDER-EMAIL>**
  
  Defines the sender’s e-mail address. This is the from address on notification e-mails.
  
  - `<SENDER-EMAIL>` – Specify the sender’s e-mail address (should not exceed 64 characters in length). Use the `email-notification > recipient > <EMAIL-ADDRESS>` command to configure the recipient’s address.

- **port <1-65535>**
  
  This option is recursive and applicable to the ‘security’ and ‘username’ parameters. Configures the SMTP server port. Use this option to configure a non-standard SMTP port on the outgoing SMTP server. The standard SMTP port is 25.
  
  - `<1-65535>` – Specify the port from 1 - 65535.
Examples

rfs7000-37FABE(config-profile-default-rfs7000)#email-notification recipient test@examplecompany.com
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
dscp-mapping 20 priority 7
no autoinstall configuration
no autoinstall firmware
............................................................
interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  use firewall-policy default
  email-notification recipient test@examplecompany.com
service pm sys-restart
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

| no | Disables or reverts settings to their default |
7.1.25 enforce-version

Profile Config Commands

Enables checking of a device’s firmware version before attempting adoption or clustering

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

enforce-version [adoption|cluster] [full|major|minor|none|strict]

Parameters

- enforce-version [adoption|cluster] [full|major|minor|none|strict]

<table>
<thead>
<tr>
<th>adoption</th>
<th>Verifies firmware versions before adopting. This option is enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Verifies firmware versions before clustering. This option is enabled by default.</td>
</tr>
<tr>
<td>full</td>
<td>Allows adoption or clustering when the first four octets of the firmware versions match (for example 5.8.1.0)</td>
</tr>
<tr>
<td>major</td>
<td>Allows adoption or clustering when the first two octets of the firmware versions match (for example 5.8)</td>
</tr>
<tr>
<td>minor</td>
<td>Allows adoption or clustering when the first three octets of the firmware versions match (for example 5.8.1)</td>
</tr>
<tr>
<td>none</td>
<td>Allows adoption or clustering between any firmware versions</td>
</tr>
<tr>
<td>strict</td>
<td>Allows adoption or clustering only when firmware versions exactly match (for example 5.8.1.0-028D). This is the default setting for both ‘adoption’ and ‘cluster’ options.</td>
</tr>
</tbody>
</table>

Examples

nx4500-5CFA2B(config-profile-testNX45XX)#enforce-version cluster full
nx4500-5CFA2B(config-profile-testNX45XX)#enforce-version adoption major

nx4500-5CFA2B(config-profile-testNX45XX)#show context
profile nx45xx testNX45XX
slot 1
slot 2

use firewall-policy default
enforce-version adoption major
enforce-version cluster full
service pm sys-restart
router ospf
router bgp
dot1x system-auth-control
dot1x use aaa-policy test
service fast-switching
nx4500-5CFA2B(config-profile-testNX45XX)#

Related Commands

no | Disables or reverts settings to their default
7.1.26 environmental-sensor

Profile Config Commands

Configures the environmental sensor settings

An AP8132 sensor module is a USB environmental sensor extension to an AP8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP8132's radio coverage area.

Supported in the following platforms:
- Access Points — AP8132

Syntax

environmental-sensor [humidity|light|motion|polling-interval|temperature]

environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]

environmental-sensor light {holdtime|radio-shutdown|threshold}

environmental-sensor light {holdtime <10-201>|radio-shutdown [all|radio-1|radio-2]}

environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}  

Parameters

- environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]

<table>
<thead>
<tr>
<th>environmental-sensor</th>
<th>Configures environmental sensor settings on this profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>humidity</td>
<td>Enables (turns on) humidity sensors. This setting is enabled by default.</td>
</tr>
<tr>
<td>motion</td>
<td>Enables (turns on) motion sensors. This setting is enabled by default.</td>
</tr>
</tbody>
</table>
| polling-interval <1-100> | Configures polling interval, in seconds, on all sensors. This is the interval after which the sensor module polls its environment to assess the various parameters, such as light intensity.  
  - <1-100> – Specify a value from 1 - 100 seconds. The default is 5 seconds. |
| temperature           | Enables (turns on) temperature sensors. This setting is enabled by default. |

- environmental-sensor light {holdtime <10-201>|radio-shutdown [all|radio-1|radio-2]}

<table>
<thead>
<tr>
<th>environmental-sensor</th>
<th>Configures environmental sensor settings on this profile</th>
</tr>
</thead>
</table>
| light                 | Enables (turns on) light sensors and specifies its settings  
  When enabled, the sensor module polls the environment to determine the light intensity.  
  Based on the reading, the system determines whether the AP8132's deployment location has lights on or off. Light intensity also helps determine whether the access point's deployment location is currently populated with clients. |
| holdtime <10-201>     | Optional. Configures a holdtime, in seconds, for the light sensor  
  - <10-201> – Specify a value from 10 - 201 seconds. The default value is 11 seconds. |
| radio-shutdown [all|radio1|radio2] | Optional. Shuts down the sensor’s radios  
  - all – Shuts down all radios. This is the default setting.  
  - radio1 – Shuts down radio 1 |

Contd..
 environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}

<table>
<thead>
<tr>
<th>environmental-sensor</th>
<th>Configures environmental sensor settings on this profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>light</td>
<td>Enables (turns on) light sensors and specifies its settings</td>
</tr>
<tr>
<td>threshold</td>
<td>Optional. Configures the upper and lower thresholds for the amount of light in the environment</td>
</tr>
<tr>
<td>high &lt;100-10000&gt;</td>
<td>Specifies the upper threshold from 100 - 10000 lux. This value determines whether lighting is on in the AP8132's deployment location. The radios are turned off if the average reading value is lower than the value set here. The default is 400 lux. <strong>Note:</strong> The light sensor triggers an event if the amount of light exceeds the specified value.</td>
</tr>
<tr>
<td>low &lt;0-1000&gt;</td>
<td>Specifies the lower threshold from 0 - 1000 lux. This value determines whether lighting is off in the AP8132's deployment location. The radios are turned on when the average value is higher than the value set here. The default is 200 lux. <strong>Note:</strong> The light sensor triggers an event if the amount of light drops below the specified value.</td>
</tr>
</tbody>
</table>

**Examples**

rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor humidity
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor polling-interval 60
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light radio-shutdown all
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light threshold high 300
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light threshold low 100
rfs4000-229D58(config-profile-testRFS4000)#show context

```
profile rfs4000 testRFS4000
  bridge vlan 1
tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
  environmental-sensor polling-interval 60
  environmental-sensor light threshold high 300
  environmental-sensor light threshold low 100
  environmental-sensor light radio-shutdown all
no autoinstall configuration
no autoinstall firmware
device-upgrade persist-images
--More--
rfs4000-229D58(config-profile-testRFS4000)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the environmental sensor's settings</td>
</tr>
</tbody>
</table>
### 7.1.27 events

**Profile Config Commands**

Displays system event messages

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
events [forward on|on]
```

**Parameters**

- `events [forward on|on]`

<table>
<thead>
<tr>
<th>forward on</th>
<th>Forwards system event messages to the wireless controller, service platform, or cluster members. This feature is enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• on – Enables forwarding of system events</td>
</tr>
<tr>
<td>on</td>
<td>Generates system events. This feature is enabled by default.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#events forward on
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

| no         | Disables or reverts settings to their default                                                                 |
### 7.1.28 export

**Profile Config Commands**

Enables export of startup.log file after every boot

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
export startup-log [max-retries|retry-interval|url]
export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]
```

**Parameters**

- `export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]`

<table>
<thead>
<tr>
<th>export startup-log</th>
<th>Enables export of the startup.log file after every boot. This option is disabled by default.</th>
</tr>
</thead>
</table>
| max-retries <2-65535> | Configures the maximum number of retries in case the export process fails  
| | • <2-65535> – Specify a value from 2 - 65535. |
| retry-interval <30-86400> | Configures the interval between two consecutive retries  
| | • <30-86400> – Specify a value from 30 - 864000 seconds. |
| url <URL> | Configures the destination URL in the following format:  
| | tftp://<hostname|IP>:<port>/path/file  
| | ftp://<user>:<passwd>@<hostname|IP>:<port>/path/file  
| | sftp://<user>@<hostname|IP>:/path/file |

**Examples**

```
nx4500-5CFA2B(config-profile-testNX45XX)#export startup-log max-retries 10 retry-interval 30 url test@examplecompany.com
```

```
nx4500-5CFA2B(config-profile-testNX45XX)#show context
profile nx45xx testNX45XX
slot 1
slot 2
...............................
interface wwan1
interface pppoe1
use firewall-policy default
**export startup-log max-retries 10 retry-interval 30 url test@examplecompany.com**
```

**Related Commands**

| `no` | Disables export of startup.log file |
7.1.29 file-sync

Profile Config Commands

Configures parameters enabling auto syncing of PKCS#12 certificate between the staging-controller and adoptee AP6522/AP6562 client bridges

This command is applicable to the access point’s profile as well as device configuration modes.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

file-sync [auto|count <1-20>]

Parameters

- file-sync [auto|count <1-20>]

| file-sync [auto|count <1-20>] | Configures the following file-synching parameters:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• auto – Enables the staging controller to autoinstall PKCS#12 certificate on a new layer 2 AP6522/AP6562 client bridge, when it comes up for the first time and adopts to the controller. The PKCS#12 certificate is installed only if the client bridge is using EAP-TLS authentication. Prior to enabling file syncing, ensure that the PKCS#12 certificate is present on the staging controller. To upload the certificate on the controller, in the user or privilege executable modes, execute the following command: file-sync &gt; load-file &gt; &lt;URL&gt;. For more information, see file-sync.</td>
</tr>
<tr>
<td></td>
<td>• count &lt;1-20&gt; – Configures the maximum number of access points that can be concurrently autoinstalled.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-20&gt; – Specify a value from 1 - 20. The default is 10 access points.</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-profile-default-rfs6000)#file-sync auto

nx9500-6C8809(config-profile-default-rfs6000)#file-sync count 8

nx9500-6C8809(config-profile-default-rfs6000)#show context profile rfs6000 default-rfs6000
no autoinstall configuration
no autoinstall firmware
no device-upgrade auto
file-sync count 8
file-sync auto
crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
--More--
nx9500-6C8809(config-profile-default-rfs6000)#

Related Commands

no
Disables automatic syncing of PKCS#12 certificate between the staging-controller and adoptee AP6522/AP6562 client bridges
7.1.30 floor

**Profile Config Commands**

Sets the floor name where the target device (access point, wireless controller, or service platform using this profile) is physically located. Assigning a building floor name helps in grouping devices within the same general coverage area.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
floor <WORD> {<1-4094>}
```

**Parameters**

- `floor <WORD> {<1-4094>}`

<table>
<thead>
<tr>
<th>floor &lt;WORD&gt; {&lt;1-4094&gt;}</th>
<th>Sets the floor name where the target device is located</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the floor name (should not exceed 64 characters in length).</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Optional. Configures the floor number from 1 - 4094. The default is 1.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#floor fifth
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
  area Ecospace
floor fifth
autoinstall configuration
autoinstall firmware
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

| **no** | Resets the configured floor name and number |
### 7.1.31 gre

**Profile Config Commands**

The following table summarizes commands that allow you to enter the GRE configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>gre</td>
<td>Enables GRE tunneling on a profile/device This command also creates a GRE tunnel and enters its configuration mode. Use this command to modify an existing GRE tunnel’s settings.</td>
<td>page 7-151</td>
</tr>
<tr>
<td>gre-config-instance</td>
<td>Summarizes GRE tunnel configuration mode commands</td>
<td>page 7-153</td>
</tr>
</tbody>
</table>
7.1.31.1 gre

Enables Generic Routing Encapsulation (GRE) tunneling on this profile, and creates a new GRE tunnel or modifies an existing GRE tunnel.

The GRE protocol allows encapsulation of one protocol over another. It is a tunneling protocol that transports any layer 3 protocol over an IP network. When enabled, a payload packet is first encapsulated in the GRE protocol. The GRE encapsulated payload is then encapsulated in another IP packet before being forwarded to the destination.

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote end point is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. Access Points can reach both the GRE peer as well as the RADIUS server using IPv4.

The WiNG software now supports for both IPv4 or IPv6 tunnel endpoints. However, a tunnel needs to contain either IPv4 or IPv6 formatted device addresses and cannot be mixed. With the new IPv6 tunnel implementation, all outbound packets are encapsulated with the GRE header, then the IPv6 header. The header source IP address is the local address of the IPv6 address of tunnel interface, and the destination address peer address of the tunnel. All inbound packets are de-capsulated by removing the IPv6 and GRE header before sending it over to the IP stack.

**NOTE:** Only one GRE tunnel can be created for every profile.

---

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

gre tunnel <GRE-TUNNEL-NAME>

**Parameters**

- gre tunnel <GRE-TUNNEL-NAME>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gre tunnel &lt;GRE-TUNNEL-NAME&gt;</td>
<td>Creates a new GRE tunnel or modifies an existing GRE tunnel</td>
</tr>
<tr>
<td></td>
<td>• &lt;GRE-TUNNEL-NAME&gt; – If creating a new tunnel, specify a unique name for it. If modifying an existing tunnel, specify its name.</td>
</tr>
</tbody>
</table>
Examples

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#?

GRE Tunnel Mode commands:
- dscp: Differentiated Services Code Point
- establishment-criteria: Set tunnel establishment criteria
- failover: L2gre tunnel failover
- mtu: L2GRE tunnel endpoint maximum transmission unit (MTU)
- native: Native trunking characteristics
- no: Negate a command or set its defaults
- peer: L2GRE peer
- tunneled-vlan: VLANs to tunnel
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#peer 1 ip 192.168.13.8
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#peer 2 ip 192.168.13.10

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
peer 1 ip 192.168.13.8
peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
bridge vlan 1
tunnel-over-level2
ip igmp snooping
ip igmp snooping querier

...............................................................
use firewall-policy default
service pm sys-restart
router ospf
gre tunnel testGREtunnel
peer 1 ip 192.168.13.8
peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile-testRFS4000)#

Related Commands

| no | Disables GRE tunneling on this profile |
The following table summarizes GRE tunnel configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp</td>
<td>Sets the GRE tunnel's Differentiated Services Code Point (DSCP) / 802.1q priority value</td>
<td>page 7-154</td>
</tr>
<tr>
<td>establishment-criteria</td>
<td>Configures the GRE tunnel establishment criteria</td>
<td>page 7-154</td>
</tr>
<tr>
<td>failover</td>
<td>Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable</td>
<td>page 7-156</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the maximum transmission unit (MTU) for IPv4/IPv6 L2GRE tunnel endpoints</td>
<td>page 7-157</td>
</tr>
<tr>
<td>native</td>
<td>Configures native trunking settings for this GRE tunnel</td>
<td>page 7-158</td>
</tr>
<tr>
<td>no</td>
<td>Removes the GRE tunnel settings based on the parameters passed</td>
<td>page 7-159</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the GRE tunnel’s end-point peers</td>
<td>page 7-160</td>
</tr>
<tr>
<td>tunneled-vlan</td>
<td>Defines the VLAN that connected clients use to route GRE-tunneled traffic within their respective WLANs</td>
<td>page 7-161</td>
</tr>
</tbody>
</table>
7.1.31.2.1 dscp

> gre-config-instance

Sets the GRE tunnel's DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
dscp [<0-63>|reflect]
```

Parameters

```
• dscp [<0-63>|reflect]
```

<table>
<thead>
<tr>
<th>dscp &lt;0-63&gt;</th>
<th>Specifies the DSCP 802.1q priority value for outer packets from 0 - 63. The default is 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp reflect</td>
<td>Copies the DSCP 802.1q value from inner packets</td>
</tr>
</tbody>
</table>

Examples

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#dscp 20
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context
gre tunnel testGRETunnel
dscp 20
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

The following example configures a GRE tunnel on a profile:

```
nx4500-5CFA2B(config-profile testNX45XX-gre-tunnel-testGRETunnel)#dscp 20
```

```
nx4500-5CFA2B(config-profile testNX45XX-gre-tunnel-testGRETunnel)#show context
gre tunnel testGRETunnel
dscp 20
```

```
nx4500-5CFA2B(config-profile testNX45XX-gre-tunnel-testGRETunnel)#
```

Related Commands

```
no
```

Removes the GRE tunnel settings based on the parameters passed
7.1.31.2.2 establishment-criteria

**gre-config-instance**

Configures the GRE tunnel establishment criteria

In a multi-controller RF domain, it is always the master node that establishes the tunnel. The tunnel is created only if the tunnel device is designated as one of the following: vrrp-master, cluster-master, or rf-domain-manager.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]

**Parameters**
- establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]

| establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>] | Configures the GRE tunnel establishment criteria. The options are: |
|---|---|
| always | - Always automatically establishes tunnel (default setting). The tunnel device need not be a cluster master, RF Domain manager, or VRRP master to establish the GRE tunnel. This is the default setting. |
| cluster-master | - Establishes tunnel only if the tunnel device is designated as the cluster master |
| rf-domain-manager | - Establishes tunnel only if the tunnel device is designated as the RF Domain manager |
| vrrp-master <1-255> | - Establishes tunnel only if the tunnel device is designated as the Virtual Router Redundancy (VRRP) master |
| <1-255> | - Configures the VRRP group ID from 1 - 255. A VRRP group enables the creation of a group of routers as a default gateway for redundancy. Clients can point to the IP address of the VRRP virtual router as their default gateway and utilize a different group member if a master becomes unavailable |

**Examples**

nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#establishment-criteria rf-domain-manager

nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel

establishment-criteria rf-domain-manager

nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#
7.1.31.2.3 failover

This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
failover interval <1-250> retry <0-10>

Parameters
- failover interval <1-250> retry <0-10>

Examples
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context gre tunnel testGRETunnel
dscp 20
   failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#

Related Commands
- no
  Removes the GRE tunnel settings based on the parameters passed
7.1.31.2.4 mtu

### gre-config-instance

Configures the MTU for IPv4/IPv6 L2GRE tunnel endpoints

The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the configured MTU are divided into smaller packets before transmission. Larger the MTU greater is the efficiency because each packet carries more user data, while protocol overheads, such as headers or underlying per-packet delays remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mtu [ipv4 <900-1476>|ipv6 <1236-1456>]
```

**Parameters**

- mtu [ipv4 <900-1476>|ipv6 <1236-1456>]

| mtu [ipv4 <900-1476>]
<table>
<thead>
<tr>
<th>ipv6 &lt;1236-1456&gt;]</th>
<th>Configures the MTU for L2GRE tunnel endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 &lt;900-1476&gt;</td>
<td>• ipv4 &lt;900-1476&gt; – Configures IPv4 L2GRE tunnel endpoint MTU from 900 - 1476. The default is 1476.</td>
</tr>
<tr>
<td>ipv6 &lt;1236-1456&gt;</td>
<td>• ipv6 &lt;1236-1456&gt; – Configures IPv6 L2GRE tunnel endpoint MTU from 1236 - 1456. The default is 1456.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#mtu ipv4 1200
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#mtu ipv6 1300
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
    mtu ipv4 1200
    mtu ipv6 1300
    establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#
```
### 7.1.31.2.5 native

**gre-config-instance**

Configures native trunking settings for this GRE tunnel

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`native [tagged|vlan <1-4094>]`

**Parameters**

- `native [tagged|vlan <1-4094>]`

<table>
<thead>
<tr>
<th>native tagged</th>
<th>Enables native VLAN tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>native vlan &lt;1-4094&gt;</th>
<th>Specifies a numerical VLAN ID (1 - 4094) for the native VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN, when no 802.1q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#native tagged
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#native vlan 20

nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
native vlan 20
native tagged
mtu ipv4 1200
mtu ipv6 1300
establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9000-gre-tunnel-testGREtunnel)#
```

**Related Commands**

- `no` Removes the GRE tunnel settings based on the parameters passed
7.1.31.2.6 no

Removes or resets the GRE tunnel settings based on the parameters passed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [dscp|establishment-criteria|failover|mtu|native|peer|tunneled-vlan]

no dscp

no establishment-criteria

no failover

no mtu [ipv4|ipv6]

no native [tagged|vlan]

no peer <1-2>

**Parameters**

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes or resets the GRE tunnel’s settings based on the parameters passed</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the GRE tunnel ‘testGRETunnel’ settings before the no commands are executed:

```plaintext
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context
gre tunnel testGRETunnel
peer 1 ip 192.168.13.6
  native vlan 1
tunneled-vlan 1,10
  native tagged
dscp 20
fallover interval 200 retry 5
```

```plaintext
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no dscp
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no native vlan
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no tunneled-vlan
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#no failover
```

The following example shows the GRE tunnel ‘testGRETunnel’ settings after the no commands are executed:

```plaintext
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context
gre tunnel testGRETunnel
peer 1 ip 192.168.13.6
  native tagged
```

```plaintext
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```
7.1.31.2.7 peer

*gre-config-instance*

Adds the GRE tunnel's end-point peers. A maximum of two peers, representing the tunnel's end points, can be added for each GRE tunnel.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

peer <1-2> ip <IPv4/IPv6>

**Parameters**

- **peer <1-2> ip <IPv4/IPv6>**

<table>
<thead>
<tr>
<th>peer &lt;1-2&gt; ip &lt;IPv4/IPv6&gt;</th>
<th>Configures the tunnel's end-point peers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-2&gt; – Specify a numeric index for each peer to help differentiate the tunnel end points.</td>
</tr>
<tr>
<td></td>
<td>• ip – Specify the IP address (IPv4/IPv6) of the added GRE peer to serve as a network address identifier.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IPv4/IPv6&gt; – Specify the peer's IPv4 or IPv6 address.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#peer 1 ip 192.168.13.6
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context gre tunnel testGRETunnel peer 1 ip 192.168.13.6 native tagged dscp 20 failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

**Related Commands**

*no* | Removes the GRE tunnel settings based on the parameters passed
7.1.31.2.8 tunneled-vlan

*gre-config-instance*

Defines the VLAN that connected clients use to route GRE tunneled traffic within their respective WLANs

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`tunneled-vlan <VLAN-ID>`

**Parameters**

- `tunneled-vlan <VLAN-ID>`

<table>
<thead>
<tr>
<th>tunneled-vlan &lt;VLAN-ID&gt;</th>
<th>Specifies the VLANs associated with this GRE tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <code>&lt;VLAN-ID&gt;</code> – Specify the VLAN IDs. Specify a comma-separated list of IDs, to specify multiple VLANs. For example, 1,10,12,16-20.</td>
</tr>
</tbody>
</table>

**Examples**

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#tunneled-vlan 10

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context
gre tunnel testGRETunnel
  peer 1 ip 192.168.13.6
  native vlan 1
tunneled-vlan 1,10
  native tagged
dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#

**Related Commands**

| no | Removes the GRE tunnel settings based on the parameters passed |
### 7.1.32 http-analyze

**Profile Config Commands**

Enables HTTP analysis on this profile. Use this command to configure the mode and interval at which data is sent to the controller (running the HTTP analytics engine).

In a hierarchically organized network, HTTP analytics data forwarding is a simple and transparent process. The site controllers (RFS4000, RFS6000, RFS7000, NX45XX, and NX65XX) receive the HTTP data from adopted APs. This data is compressed and forwarded to the *Network Operations Center* (NOC) controller. The NOC controller caches, formats, and uploads this information to the external analytics engine. There is no need for a separate configuration to enable this feature.

For more information on the hierarchical network, see *device-upgrade*.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

```
http-analyze [compress|update-interval <1-3600>]
```

**Parameters**

- `http-analyze [compress|update-interval <1-3600>]`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http-analyze</code></td>
<td>Configures HTTP analysis parameters. These parameters are: compress and update-interval.</td>
</tr>
<tr>
<td><code>compress</code></td>
<td>Compresses update files before forwarding to the controller. This option is disabled by default.</td>
</tr>
<tr>
<td><code>update-interval</code></td>
<td>Sets the interval, in seconds, at which buffered packets are pushed to analyze the HTTP data</td>
</tr>
<tr>
<td><code>&lt;1-3600&gt;</code></td>
<td>- Specify the interval from 1 - 3600 seconds. The default is 60 seconds.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#http-analyze compress
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#http-analyze update-interval 200
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
    ip igmp snooping
    ip igmp snooping querier
    autoinstall configuration
    autoinstall firmware
    crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
    crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  .
  .
  qos trust 802.1p
  interface pppoe1
  use firewall-policy default
  http-analyze update-interval 200
  http-analyze compress
  service pm sys-restart
  router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables HTTP analyze settings</td>
</tr>
</tbody>
</table>
7.1.33 **http-analyze (NX45XX, NX65XX, and NX9000)**

*Profile Config Commands*

Enables forwarding of HTTP request related data to the HTTP analytics engine.

Wireless clients (MUs) connect to APs and route their HTTP requests through the APs. These APs extract and forward HTTP request packets, through MiNT, to the NX series controller. The NX series controller uses a new analytic daemon to cache, format, and forward information to the analytics engine. Currently the analytics daemon is supported only on the NX series service platform. Therefore, it is essential that all APs should use an NX series service platform as controller.

In a hierarchically organized network, HTTP analytics data forwarding is a simple and transparent process. The site controllers (RFS4000, RFS6000, RFS7000, NX45XX, and NX65XX) receive the HTTP data from adopted APs adopted. This data is compressed and forwarded to the *Network Operations Center* (NOC) controller. There is no need for a separate configuration to enable this feature.

Use this command to configure the mode and interval at which data is sent to the controller and the external analytics engine. This command also configures the external engine’s details, such as URL, credentials etc.

A NX9500 and NX9510 model service platforms (NOC) can provide granular and robust analytic reporting for a RFS4000, RFS6000 or RFS7000 controller managed network or a NX45XX/NX65XX service platform managed network. You can use the analytics feature Using analytics, data is collected at administrator defined intervals.

Analytics can parse and process Smart RF events within the NOC managed network as events are received. When a Smart RF event occurs, the analytics engine parses the new channel and power information from the Smart RF event, as opposed to retrieving the event from the devices themselves.

The analytics user interface populates information within a *data store*, with multiple displays partitioned by performance function. The data store is a customizable display managed with just the content the administrator wants viewed. The data store is purged after 90 days if no administration is conducted sooner.

A separate hot spare analytics license is enforced at the NOC. The license restricts the number of Access Point streams processed at the NOC or forwarded to partner systems for further processing. The analytics feature can be turned on at select APs by enabling them in configuration. This way the customer can enable analytics on a select set of APs and not the entire system as long as the number of APs on which it is enabled is less than or equal to the total number of AP analytics licenses available at the NOC controller.

---

**NOTE:** The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors.

---

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
http-analyze [compress|controller|external-server|update-interval]

http-analyze [compress|controller|update-interval <1-3600>]

http-analyze external-server [password|proxy|update-interval|url|username|validate-server-certificate]

http-analyze external-server [password <WORD>|proxy <URL>|update-interval <1-3600>|url <URL> |username <WORD>|validate-server-certificate]
```
### Parameters

- **http-analyze [compress|controller|update-interval <1-3600>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>http-analyze</strong></td>
<td>Configures HTTP analysis related parameters</td>
</tr>
<tr>
<td><strong>compress</strong></td>
<td>Compresses update files before forwarding to the controller. This option is disabled by default.</td>
</tr>
<tr>
<td><strong>controller</strong></td>
<td>Sends the collected analytics data to the controller (data is forwarded to a local analytics engines on the NX series service platform)</td>
</tr>
<tr>
<td><strong>update-interval</strong></td>
<td>Configures the interval, in seconds, at which buffered packets are pushed to the controller</td>
</tr>
<tr>
<td><strong>&lt;1-3600&gt;</strong></td>
<td>• &lt;1-3600&gt; – Specify the interval from 1 - 3600 seconds. The default is 60 seconds.</td>
</tr>
</tbody>
</table>

- **http-analyze external-server [password <WORD>|proxy <URL>|update-interval|url|username|validate-server-certificate]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>http-analyze external-server</strong></td>
<td>Configures the external HTTP analytics engine’s parameters</td>
</tr>
<tr>
<td><strong>password &lt;WORD&gt;</strong></td>
<td>Configures the external analytics engine’s password</td>
</tr>
<tr>
<td><strong>&lt;WORD&gt;</strong></td>
<td>• &lt;WORD&gt; – Provide the login password. This is the password associated with the user name needed to access the external analytics engine.</td>
</tr>
<tr>
<td><strong>proxy &lt;URL&gt;</strong></td>
<td>Configures the proxy server’s uniform resource locator (URL)</td>
</tr>
<tr>
<td><strong>&lt;URL&gt;</strong></td>
<td>• &lt;URL&gt; – Specify the proxy server’s URL in the following format:</td>
</tr>
<tr>
<td></td>
<td><a href="http://username:password@proxy-server:port">http://username:password@proxy-server:port</a>. For example, <a href="http://mot:sym@wwwgate0.mot.com:1080">http://mot:sym@wwwgate0.mot.com:1080</a></td>
</tr>
<tr>
<td><strong>update-interval</strong></td>
<td>Configures the interval, in seconds, at which buffered packets are pushed to the external analytics engine</td>
</tr>
<tr>
<td><strong>&lt;1-3600&gt;</strong></td>
<td>• &lt;1-3600&gt; – Specify the interval from 1 - 3600 seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td><strong>url &lt;URL&gt;</strong></td>
<td>Configures the external analytics engine’s IP address or URL</td>
</tr>
<tr>
<td><strong>&lt;URL&gt;</strong></td>
<td>• &lt;URL&gt; – Provide the IP address or URL.</td>
</tr>
<tr>
<td><strong>username &lt;WORD&gt;</strong></td>
<td>Configures the user name needed to access the external analytics engine</td>
</tr>
<tr>
<td><strong>&lt;WORD&gt;</strong></td>
<td>• &lt;WORD&gt; – Provide the user name.</td>
</tr>
<tr>
<td><strong>validate-server-certificate</strong></td>
<td>Validates the external analytics engine’s certificate, if it is using HTTPS as the mode of access</td>
</tr>
</tbody>
</table>

### Examples

- `nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#http-analyze external-server username anonymous`
- `nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#http-analyze external-server password anonymous`
- `nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#http-analyze external-server validate-server-certificate`
- `nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#http-analyze external-server update-interval 100`
- `nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#show context`
- `nx45xx B4-C7-99-5C-FA-2B`
  - use profile default-nx45xx
  - use rf-domain default
  - hostname nx4500-5CFA2B
  - license AP DEFAULT-12AP-LICENSE
license ADSEC DEFAULT-ADV-SEC-LICENSE
ip default-gateway 192.168.13.2
interface up1
   no shutdown
   switchport mode access
   switchport access vlan 1
interface vlan1
   ip address 192.168.13.12/24
logging on
logging console warnings
logging buffered warnings
http-analyze external-server url https://192.168.13.10
http-analyze external-server username anonymous
http-analyze external-server password anonymous
http-analyze external-server validate-server-certificate
http-analyze external-server update-interval 100

Related Commands

| no     | Disables HTTP analytics settings on an NX series service platform |
7.1.34 interface

Profile Config Commands

The following table summarizes interface configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Selects an interface to configure</td>
<td>page 7-168</td>
</tr>
</tbody>
</table>
| interface-config-
  instance            | Summarizes Ethernet interface (associated with the wireless controller or   | page 7-172 |
|                       | service platform) configuration commands                                   |             |
| interface-config-
  vlan-instance        | Summarizes VLAN interface configuration commands                            | page 7-200 |
| interface-config-
  radio-instance       | Summarizes radio interface configuration commands (applicable to devices   | page 7-218 |
|                       | with built-in radios)                                                       |             |
| interface-config-
  wwan-instance        | Summarizes WWAN interface configuration commands                            | page 7-297 |
| interface-config-
  serial-instance      | Summarizes serial interface configuration commands (supported only on the  | page 7-308 |
|                       | NX45XX and NX65XX series service platform profiles)                         |             |
| interface-config-
  t1e1-instance        | Summarizes the T1E1 interface configuration commands (supported only on    | page 7-323 |
|                       | the NX45XX and NX65XX series service platform profiles)                     |             |
| interface-config-
  vm-instance          | Summarizes the virtual machine interface configuration commands            | page 7-336 |
|                       | (supported only on the NX45XX and NX65XX series service platform profiles)   |             |
7.1.34.1 interface

Selects an interface to configure

A profile’s interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to RFS4000, RFS6000, RFS7000 controllers and NX4500, NX6500, NX7500 and NX9000 series service platforms. Ports vary depending on the platform, but controller or service platform models do have some of the same physical interfaces.

A controller or service platform requires its virtual interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each VLAN ID the controller or service platform is connected to.

If the profile is configured to support an access point radio, an additional radio interface is available, unique to the access point’s radio configuration.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax Service Platforms

interface [<INTERFACE-NAME>|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]|serial <1-4>|t1e1 <1-4>|up <1-2>|vlan <1-4094>|vmif <1-12>|wwan1|xge <1-4>]

Syntax Access Points and Wireless Controllers

interface [<INTERFACE-NAME>|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]|up1|vlan <1-4094>|vmif <1-8>|wwan1|xge <1-4>]

Parameters

<table>
<thead>
<tr>
<th>&lt;INTERFACE-NAME&gt;</th>
<th>Enters the configuration mode of the interface identified by the &lt;INTERFACE-NAME&gt; keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe &lt;1-4&gt;</td>
<td>Selects a FastEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4&gt; – Specify the interface index from 1 - 4.</td>
</tr>
<tr>
<td></td>
<td>This interface is applicable only for AP6511 model controller.</td>
</tr>
<tr>
<td>ge &lt;1-24&gt;</td>
<td>Selects a GigabitEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-24&gt; – Specify the interface index from 1 - 24. (4 for RFS7000 and 8 for RFS6000).</td>
</tr>
<tr>
<td></td>
<td>The NX45XX and NX65XX series service platforms have 24 GigabitEthernet interface ports.</td>
</tr>
<tr>
<td>me1</td>
<td>Selects a management interface</td>
</tr>
<tr>
<td></td>
<td>Not applicable for RFS4000 model devices.</td>
</tr>
<tr>
<td></td>
<td>The management interface is applicable only for RFS6000 and RFS7000 model controllers.</td>
</tr>
<tr>
<td>port-channel &lt;1-4&gt;</td>
<td>Selects the port channel interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4&gt; – Specify the interface index from 1 - 4.</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Selects the PPP over Ethernet interface to configure</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radio [1</td>
<td>2</td>
</tr>
<tr>
<td>serial &lt;1-4&gt;</td>
<td>Selects a serial interface&lt;br&gt;• &lt;1-4&gt; – Specify the interface index from 1 - 4.&lt;br&gt;The serial interfaces are virtual interfaces available only on the NX45XX and NX65XX series service platforms.</td>
</tr>
<tr>
<td>t1e1 &lt;1-4&gt;</td>
<td>Selects the T1 and E1 slot interfaces&lt;br&gt;• &lt;1-4&gt; – Specify the T1 or E1 slot ID from 1 - 4.&lt;br&gt;The T1E1 interfaces are available only on the NX45XX and NX65XX series service platforms.</td>
</tr>
<tr>
<td>up1</td>
<td>Selects the uplink GigabitEthernet interface&lt;br&gt;The NX45XX and NX65XX series profiles support 2 uplink interfaces (up &lt;1-2&gt;).</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Selects a VLAN interface&lt;br&gt;• &lt;1-4094&gt; – Specify the SVI VLAN ID from 1 - 4094.</td>
</tr>
<tr>
<td>vmif &lt;1-8&gt;</td>
<td>Selects the virtual machine (VM) interface&lt;br&gt;• &lt;1-8&gt; – Specify the VM interface index from 1 - 8.&lt;br&gt;The VM interfaces are available only on the NX45XX, NX65XX, NX9XXX series service platforms.</td>
</tr>
<tr>
<td>wwan1</td>
<td>Selects a Wireless WAN interface&lt;br&gt;This interface is applicable only to AP71XX, AP81XX, AP82XX, RFS4000, RFS6000 model access points and controllers.</td>
</tr>
<tr>
<td>xge &lt;1-4&gt;</td>
<td>Selects a TenGigabitEthernet interface&lt;br&gt;• &lt;1-2&gt; – Specify the interface index from 1 - 4.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ports available on a device vary depending on the model. The following ports are available on RFS4000, RFS6000 and RFS7000 model wireless controllers:

- RFS4000 - ge1, ge2, ge3, ge4, ge5, up1
- RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1
- RFS7000 - ge1, ge2, ge3, ge4, me1

GE ports on are RJ-45 supporting 10/100/1000Mbps. GE ports on the RFS7000 can be RJ-45 or fiber ports supporting 10/100/1000Mbps.

ME ports are available on RFS6000 and RFS7000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

The ports available on service platforms also vary depending on the model. The following ports are available on NX series service platforms:

- NX4500 - up1, up2
- NX4524 - ge1-ge24, up1, up2
- NX5500 - ge1, ge2
- NX6500 - up1, up2
- NX6524 - ge1-ge24, up1, up2
- NX7500 - ge1-ge10, xge1-xge2
- NX9000 series - ge1, ge2, xge1-xge4

GE ports are available on RFS4000, RFS6000 and RFS7000 controllers and NX4524 and NX6524 model service platforms. GE ports are RJ-45 supporting 10/100/1000Mbps. GE ports on the RFS7000 can be RJ-45 or fiber ports supporting 10/100/1000Mbps.

ME ports are available on RFS6000 and RFS7000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

UP ports are available on RFS4000 and RFS6000 platforms. A UP port is used to connect to the backbone network. UP ports are available on RFS4000 and RFS6000 controllers and NX4500 and NX6500 series service platforms. A UP port supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone as it has a non-blocking 1gbps connection unlike the GE ports.

The following ports are available on access points:
- AP6511 - fe1, fe2, fe3, fe4, up1
- AP6521 - GE1/POE (LAN)
- AP6522 - GE1/POE (LAN)
- AP6532 - GE1/POE
- AP6562 - GE1/POE
- AP7131 - GE1/POE (LAN), GE2 (WAN)
- AP7161 - GE1/POE (LAN), GE2 (WAN)
- AP7181 - GE1/POE (LAN), GE2 (WAN)
- AP7502 - GE1 (THRU), fe1, fe2, fe3,
- AP7522 - GE1/POE (LAN)
- AP7532 - GE1/POE (LAN)
- AP81XX - GE1/POE (LAN), GE2 (WAN)
- AP82XX - GE1/POE (LAN), GE2 (WAN)

**NOTE:** For a NX7500 model service platform, there are options for either a 2 port or 4 port network management card. Either card can be managed using WiNG. If the 4 port card is used, ports ge7-ge10 are available. If the 2 port card is used, ports xge1-xge2 are available.

### Examples
```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#?
```

SVI configuration commands:
- `crypto` Encryption module
- `description` Vlan description
- `dhcp` Dynamic Host Configuration Protocol (DHCP)
- `dhcp-relay-incoming` Allow on-board DHCP server to respond to relayed DHCP packets on this interface
- `ip` Interface Internet Protocol config commands
- `ipv6` Internet Protocol version 6 (IPv6)
- `no` Negate a command or set its defaults
- `shutdown` Shutdown the selected interface
- `use` Set setting to use

- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
**help**  Description of the interactive help system
**revert**  Revert changes
**service**  Service Commands
**show**  Show running system information
**write**  Write running configuration to memory or terminal

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
```

```
nx4500-5CFA2B(config-profile-testNX45XX)#interface vmif 2
nx4500-5CFA2B(config-profile-testNX45XX-if-vmif12)#
```

```
nx4500-5CFA2B(config-profile-testNX45XX-if-vmif2)#?
```

**VM Interface Mode commands:**
- **description**  Port description
- **ip**  Internet Protocol (IP)
- **ipv6**  Internet Protocol version 6 (IPv6)
- **no**  Negate a command or set its defaults
- **qos**  Quality of service
- **switchport**  Set switching mode characteristics
- **use**  Set setting to use
- **clrscr**  Clears the display screen
- **commit**  Commit all changes made in this session
- **do**  Run commands from Exec mode
- **end**  End current mode and change to EXEC mode
- **exit**  End current mode and down to previous mode
- **help**  Description of the interactive help system
- **revert**  Revert changes
- **service**  Service Commands
- **show**  Show running system information
- **write**  Write running configuration to memory or terminal

```
nx4500-5CFA2B(config-profile-testNX45XX-if-vmif2)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the selected interface</td>
</tr>
</tbody>
</table>
7.1.34.2 interface-config-instance

Use the config-profile-<PROFILE-NAME> instance to configure the Ethernet, VLAN and tunnel associated with the access point, wireless controller, or service platform.

To switch to this mode, use the following command:

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface [<INTERFACE-NAME>|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]|up1|vlan <1-4094>|wwan1|xge <1-4>]
<DEVICE>(config-profile-default-rfs7000)# ge 1
```

The following example uses the config-profile-default-rfs7000 instance to configure a GigabitEthernet interface:

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#?
```

The following table summarizes the interface configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal-enforcement</td>
<td>Enables captive-portal enforcement on this Ethernet port</td>
<td>page 7-174</td>
</tr>
<tr>
<td>cdp</td>
<td>Enables Cisco Discovery Protocol (CDP) on this Ethernet port</td>
<td>page 7-175</td>
</tr>
<tr>
<td>channel-group</td>
<td>Assigns this Ethernet port to a channel group</td>
<td>page 7-176</td>
</tr>
<tr>
<td>description</td>
<td>Configures a description for this Ethernet port</td>
<td>page 7-177</td>
</tr>
</tbody>
</table>

**NOTE:** The NX45XX and NX65XX series service platforms have 24 GigabitEthernet ports.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x (authenticator)</td>
<td>Configures 802.1X authenticator settings</td>
<td>page 7-178</td>
</tr>
<tr>
<td>dot1x (supplicant)</td>
<td>Configures 802.1X supplicant settings</td>
<td>page 7-180</td>
</tr>
<tr>
<td>duplex</td>
<td>Specifies the duplex mode for the interface</td>
<td>page 7-181</td>
</tr>
<tr>
<td>ip</td>
<td>Sets the IP address for this Ethernet port</td>
<td>page 7-182</td>
</tr>
<tr>
<td>ipv6</td>
<td>Sets the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this interface</td>
<td>page 7-183</td>
</tr>
<tr>
<td>lldp</td>
<td>Configures Link Local Discovery Protocol (LLDP)</td>
<td>page 7-185</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables MAC-based authentication on this Ethernet port</td>
<td>page 7-186</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the selected Ethernet port settings</td>
<td>page 7-187</td>
</tr>
<tr>
<td>power</td>
<td>Configures Power over Ethernet (PoE) settings on this interface</td>
<td>page 7-188</td>
</tr>
<tr>
<td>qos</td>
<td>Enables QoS</td>
<td>page 7-189</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables the selected Ethernet port</td>
<td>page 7-190</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Configures spanning tree parameters</td>
<td>page 7-191</td>
</tr>
<tr>
<td>speed</td>
<td>Specifies the speed on this Ethernet port</td>
<td>page 7-194</td>
</tr>
<tr>
<td>switchport</td>
<td>Sets interface switching mode characteristics</td>
<td>page 7-195</td>
</tr>
<tr>
<td>use</td>
<td>Associates IPv4, IPv6, and/or MAC ACL with the selected Ethernet port</td>
<td>page 7-198</td>
</tr>
</tbody>
</table>
7.1.34.2.1 captive-portal-enforcement

*interface-config-instance*

Enables application of captive portal access permission rules to data transmitted over this specific Ethernet port. This setting is disabled by default.

Captive portal enforcement allows users on the wired network to pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user can pass traffic on the captive portal.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
captive-portal-enforcement {fall-back}

**Parameters**
- captive-portal-enforcement {fall-back}

<table>
<thead>
<tr>
<th>captive-portal-enforcement</th>
<th>Enables captive-portal enforcement on this Ethernet port</th>
</tr>
</thead>
<tbody>
<tr>
<td>fall-back</td>
<td>• fall-back – Optional. Enforces captive portal validation only if port authentication fails. When selected, captive portal policies are enforced only when RADIUS authentication of the client MAC address is not successful. If this option is not selected, captive portal policies are enforced regardless of the client's MAC address being in the RADIUS server's user database or not.</td>
</tr>
</tbody>
</table>

**Examples**
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge2)#captive-portal-enforcement
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge2)#show context interface ge2 captive-portal-enforcement
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge2)#

**Related Commands**

| no | Disables captive-portal enforcement on this interface |
7.1.34.2.2 cdp

*interface-config-instance*

Enables CDP on the selected GE port

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
cdp [receive|transmit]

**Parameters**
- cdp [receive|transmit]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>receive</td>
<td>Enables CDP packet snooping on this interface. When enabled, the port receives periodic interface updates from a multicast address. This option is enabled by default.</td>
</tr>
<tr>
<td>transmit</td>
<td>Enables CDP packet transmission on this interface. When enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.</td>
</tr>
</tbody>
</table>

**Examples**
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#cdp transmit

**Related Commands**
- no Disables CDP packet snooping on the controller or service platform’s selected GE ports
7.1.34.2.3 channel-group

Assigns this Ethernet port to a channel group. Ethernet ports can be aggregated to form a channel group. For example, an RFS7000 has four (4) Ethernet ports (1, 2, 3, & 4). These can be aggregated to form a minimum of one and maximum of two channel groups. A port can be a member of only one channel group at a time.

The maximum number of channel groups supported on a device depends on the number of Ethernet ports available.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
channel-group <1-4>

Parameters
- channel-group <1-4>

Examples
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#channel-group 1

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
   interface ge1
   ip dhcp trust
   qos trust dscp
   qos trust 802.1p
   channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

Related Commands

no

Removes the channel group to which this port belongs
### 7.1.34.2.4 description

**interface-config-instance**

Configures a description for this Ethernet port.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
description [<LINE>|<WORD>]

**Parameters**
- description [<LINE>|<WORD>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;LINE&gt;</td>
<td>Configures the maximum length (number of characters) of the interface description</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>Configures a unique description for this interface. The description should not exceed the length specified by the &lt;LINE&gt; parameter.</td>
</tr>
</tbody>
</table>

**Examples**
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#description "This is GigabitEthernet interface for Royal King"
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
  description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the interface description</td>
</tr>
</tbody>
</table>
**7.1.34.2.5 dot1x (authenticator)**

`interface-config-instance`

Configures 802.1X authenticator settings

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

```
dot1x authenticator [guest-vlan <1-4094>|host-mode [multi-host|single-host]|max-reauth-req <1-10>|port-control [auto|force-authorized|force-unauthorized]|reauthenticate|timeout [quiet-period|reauth-period <1-65535>]]
```

**Parameters**

- `dot1x authenticator [guest-vlan <1-4094>|host-mode [multi-host|single-host]|max-reauth-req <1-10>|port-control [auto|force-authorized|force-unauthorized]|reauthenticate|timeout [quiet-period|reauth-period <1-65535>]]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x authenticator</td>
<td>Configures 802.1x authenticator settings</td>
</tr>
<tr>
<td>guest-vlan &lt;1-4094&gt;</td>
<td>Configures the guest VLAN for this interface. This is the VLAN, traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled. Select the VLAN index from 1 - 4094.</td>
</tr>
</tbody>
</table>
| host-mode                  | Configures the host mode for this interface  
| [multi-host|single-host]       | • multi-host – Configures multiple host mode  
| max-reauth-req <1-10>      | • single-host – Configures single host mode. This is the default setting.   |
| port-control [auto|force-authorized|force-unauthorized]| Configures maximum number of re-authorization retries for the supplicant. This is the maximum number of re-authentication attempts made before this port is moved to unauthorized.
| reauthenticate             | • <1-10> – Specify a value from 1 -10. The default is 2.                     |
| timeout [quiet-period|reauth-period <1-65535>]] |                                                                         |

---

**NOTE:** The dot1x (802.1x) supplicant settings are documented in the next section.
### port-control

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`[auto</td>
<td>force-authorized</td>
</tr>
<tr>
<td>auto</td>
<td>Configures auto port state</td>
</tr>
<tr>
<td>force-authorized</td>
<td>Configures authorized port state. This is the default setting.</td>
</tr>
<tr>
<td>force-unauthorized</td>
<td>Configures unauthorized port state</td>
</tr>
</tbody>
</table>

### reauthenticate

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enables re-authentication for this port. When enabled, clients are forced to re-authenticate on this port. The setting is disabled by default. Therefore, clients are not required to re-authenticate for connection over this port until this setting is enabled.</td>
</tr>
</tbody>
</table>

### timeout [quiet-period]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reauth-period</td>
<td>Configures timeout settings for this interface</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The following option is common to 'quiet-period' and 'reauth-period' keywords:</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Specify a 'quiet-period' or 'reauth-period' from 1 - 65535 seconds.</td>
</tr>
</tbody>
</table>

### Examples

```bash
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator guest-vlan 2
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator host-mode multi-host
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator max-reauth-req 6
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x authenticator reauthenticate
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context interface ge1
dot1x authenticator host-mode multi-host
dot1x authenticator guest-vlan 2
dot1x authenticator reauthenticate
dot1x authenticator max-reauth-count 6
ip dhcp trust
qos trust dscp
qos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.2.6 dot1x (supplicant)

interface-config-instance

Configures 802.1X supplicant (client) settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]

Parameters

- dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]

<table>
<thead>
<tr>
<th>dot1x supplicant</th>
<th>Configures 802.1x supplicant settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>username &lt;USERNAME&gt;</td>
<td>Sets the username for authentication</td>
</tr>
<tr>
<td>password [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;</td>
</tr>
<tr>
<td></td>
<td>• 0 &lt;WORD&gt; – Sets a clear text password</td>
</tr>
<tr>
<td></td>
<td>• 2 &lt;WORD&gt; – Sets an encrypted password</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the password.</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x supplicant username bob password 0 test@123

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context

interface ge1
   dot1x supplicant username bob password 0 test@123
   dot1x authenticator host-mode multi-host
   dot1x authenticator guest-vlan 2
   dot1x authenticator reauthenticate
   dot1x authenticator max-reauth-count 6
   ip dhcp trust
   qos trust dscp
   qos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#

Related Commands

- no
  Removes 802.1X supplicant (client) settings
7.1.34.2.7 duplex

> Interface-config-instance

Configures duplex mode (for the flow of packets) on this Ethernet port.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

duplex [auto|half|full]

Parameters
- duplex [auto|half|full]

<table>
<thead>
<tr>
<th>auto</th>
<th>Enables automatic duplexity on an interface port. The port automatically detects whether it should run in full or half-duplex mode. (default setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>half</td>
<td>Sets the port to half-duplex mode. Allows communication in one direction only at any given time. When selected, data is sent over the port, then immediately data is received from the direction in which the data was transmitted.</td>
</tr>
<tr>
<td>full</td>
<td>Sets the port to full-duplex mode. Allows communication in both directions simultaneously. When selected, the port can send data while receiving data as well.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#duplex full

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context

interface ge1
description This is GigabitEthernet interface for Royal King
duplex full
dot1x supplicant username Bob password 0 test@123
ip dhcp trust
gos trust dscp
gos trust 802.1p
channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

Related Commands

no | Reverts to default (auto) |
7.1.34.2.8 ip

Sets the ARP and DHCP components for this Ethernet port

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ip [arp|dhcp]

ip [arp [header-mismatch-validation|trust]|dhcp trust]

Parameters

- ip [arp [header-mismatch-validation|trust]|dhcp trust]

Examples

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#ip dhcp trust

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#ip arp header-mismatch-validation

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
interface ge1
description This is\ GigabitEthernet\ interface\ for\ Royal\ King
duplex full
dotix supplicant username Bob password 0 test@123
ip dhcp trust
ip arp header-mismatch-validation
qos trust dscp
qos trust 802.1p
channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

Related Commands

no | Removes the ARP and DHCP components configured for this interface
7.1.34.2.9 ipv6

Sets the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this interface.

The ICMPv6 ND protocol uses ICMP messages and solicited multicast addresses to track neighboring devices on the same local network. These messages are used to discover a neighbor’s link layer address and to verify if a neighboring device is reachable.

The ICMP messages are neighbor solicitation (NS) and neighbor advertisement (NA) messages. When a destination host receives an NS message from a neighbor, it replies back with a NA. The NA contains the following information:

- Source address – This is the IPv6 address of the device sending the NA
- Destination address – This is the IPv6 address of the device from whom the NS message is received
- Data portion – Includes the link layer address of the device sending the NA

NS messages are used to verify a neighbor’s (whose link layer address is known) reachability. To confirm a neighbor’s reachability a node sends an NS message in which the neighbor’s unicast address is specified as the destination address. If the neighbor sends back an acknowledgment on receipt of the NS message it is considered reachable.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ipv6 [dhcpv6|nd]
ipv6 dhcpv6 trust
ipv6 nd [header-mismatch-validation|raguard|trust]

Parameters

- ipv6 dhcpv6 trust

  Enables trust state for DHCPv6 responses on this interface. When enabled, all DHCPv6 responses received on this port are trusted and forwarded. This option is enabled by default.

  Note: A DHCPv6 server can be connected to a DHCPv6 trusted port.

- ipv6 nd [header-mismatch-validation|raguard|trust]

  Configures IPv6 ND settings

  header-mismatch-validation

  Enables matching of source MAC address in the ICMPv6 ND and Ethernet headers (link layer option) to check for mismatch. This option is disabled by default.
### Examples

```text
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 dhcpv6 trust
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 nd header-mismatch-validation
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 nd trust
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge1)#show context interface ge1
  switchport mode access
  switchport access vlan 1
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  ipv6 dhcpv6 trust
rfs7000-6DCD4B(config-device-B4-C7-99-6D-CD-4B-if-ge1)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes or reverts IPv6 settings on this interface</td>
</tr>
</tbody>
</table>

---

### raguard

Allows redirection of *router advertisements* (RAs) and ICMPv6 packets originating on this interface. When selected, RAs are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is enabled by default.

### trust

Enables trust state for IPv6 ND requests received on this interface. When enabled, IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to the request with a router advertisement packet containing Internet Layer configuration parameters. This option is disabled by default.
7.1.34.2.10 lldp

interface-config-instance

Configures Link Local Discovery Protocol (LLDP) parameters on this Ethernet port

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
lldp [receive|transmit]

Parameters
- lldp [receive|transmit]

<table>
<thead>
<tr>
<th>receive</th>
<th>Enables LLDP Protocol Data Units (PDUs) snooping. When enabled, the port receives periodic updates from a multicast address informing about presence of neighbors. This option is enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit</td>
<td>Enables LLDP PDU transmission. When enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#lldp transmit

Related Commands
- no Disables or reverts interface settings to their default
7.1.34.2.11 mac-auth

`interface-config-instance`

Enables authentication of MAC addresses on the selected wired port. When enabled, this feature authenticates the MAC address of a device, connecting to this interface, with a RADIUS server. When successfully authenticated, packets from the source are processed. Since only one MAC address is supported per wired port, packets from all other sources are dropped.

For more information on enabling this feature see, `mac-auth`.

Enable port MAC authentication in conjunction with Wired 802.1x settings to configure a MAC authentication AAA policy.

This option is also available in the device configuration mode.

Supported in the following platforms:
- Access Points — AP622, AP6522 AP6562, AP71XX, AP7502, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`mac-auth`

Parameters

None

Examples

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#mac-auth
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
interface ge1
    mac-auth
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
    channel-group 1
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
rfs4000-229D58(config-profile-testRFS4000-if-ge5)#mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
interface ge5
    switchport mode access
    switchport access vlan 1
    dot1x authenticator host-mode single-host
    dot1x authenticator guest-vlan 5
    dot1x authenticator port-control auto
    mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#
```

Related Commands

- `no` Disables authentication of MAC addresses on the selected wired port
7.1.34.2.12 no

Remove or reverts the selected Ethernet port settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
no [captive-portal-enforcement|cdp|channel-group|description|dot1x|duplex|ip|
ipv6|lldp|mac-auth|power|qos|shutdown|spanning-tree|speed|switchport|use]
```

```
no [cdp|lldp] [receive|transmit]
```

```
o dot1x [authenticator [guest-vlan|host-mode|max-reauth-req|port-control|reauthentication|timeout [quiet-period|reauth-period]]|supplicant]
o ip [arp [header-mismatch-validation|trust]|dhcp trust]
o ipv6 [dhcpv6 trust|nd [header-mismatch-validation|raguard|trust]]
```

```
o power {best-effort|limit|priority}
o qos trust [802.1p|cos|dscp]
o spanning-tree [bpdufilter|bdpuguard|force-version|guard|link-type|mst|portfast]
o switchport [access vlan|mode|trunk native tagged]
o use [ip-access-list|ipv6-access-list|mac-access-list] in
```

Parameters

- no <PARAMETERS>

```
no <PARAMETERS> Removes or reverts this Ethernet port settings based on the parameters passed
```

Usage Guidelines
The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples
```text
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no cdp
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no duplex
```
7.1.34.2.13 power

*interface-config-instance*

Configures PoE settings on this interface

When configured, this option allows the selected port to use Power over Ethernet. When enabled, the controller supports 802.3af PoE on each of its GE ports. PoE allows users to monitor port power consumption and configure power usage limits and priorities for each GE port.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
power {best-effort|limit <0-40>|priority [critical|high|low]}
```

**Parameters**

- `power {best-effort|limit <0-40>|priority [critical|high|low]}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>power</code></td>
<td>Configures power related thresholds for this interface</td>
</tr>
<tr>
<td><code>best-effort</code></td>
<td>Optional. Enables power when the device is not operating from 802.3at class 4 power source</td>
</tr>
<tr>
<td><code>limit &lt;0-40&gt;</code></td>
<td>Optional. Configures the PoE power limit from 0 - 40 Watts. The default is 30 Watts.</td>
</tr>
</tbody>
</table>
| `priority [critical|high|low]` | Optional. Configures the PoE power priority on this interface. This is the priority assigned to this port versus the power requirements of the other ports available on the controller.  
  - `critical` – Sets PoE priority as critical  
  - `high` – Sets PoE priority as high  
  - `low` – Sets PoE priority as low. This is the default setting. |

**Examples**

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#power limit 30
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#power priority critical
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
  interface ge1
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
    power limit 30
    power priority critical
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

**Related Commands**

- `no` Removes PoE settings on this interface
7.1.34.2.14 qos

```
interface-config-instance
```

Defines Quality of Service (QoS) settings on this Ethernet port

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
qos trust [802.1p|cos|dscp]
```

**Parameters**

- `qos trust [802.1p|cos|dscp]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| trust [802.1p|cos|dscp] | Trusts QoS values ingressing on this interface  
| |  
| | • 802.1p – Trusts 802.1p COS values ingressing on this interface  
| | • cos – Trusts 802.1p COS values ingressing on this interface. This option is enabled by default.  
| | • dscp – Trusts IP DSCP QOS values ingressing on this interface. This option is enabled by default. |

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#qos trust dscp
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#qos trust 802.1p
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
interface ge1
description This\ is\ GigabitEthernet\ interface\ for\ Royal\ King
duplex full
dot1x supplicant username Bob password 0 test@123
ip dhcp trust
ip arp header-mismatch-validation
qos trust dscp
qos trust 802.1p
channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

**Related Commands**

```
no
```

Removes QoS settings on the selected interface
7.1.34.2.15 shutdown

**interface-config-instance**

Shuts down (disables) an interface. The interface is administratively enabled unless explicitly disabled using this command.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```text
cfg#shutdown
```

**Parameters**

None

**Examples**

```text
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.2.16 spanning-tree

**interface-config-instance**

Configures spanning tree parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|port-cisco-interoperability|portfast]
spanning-tree [force-version <0-3>|guard root|portfast]
spanning-tree [bpdufilter|bpduguard] [default|disable|enable]
spanning-tree link-type [point-to-point|shared]
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
spanning-tree port-cisco-interoperability [disable|enable]
```

**Parameters**

- **force-version <0-3>**

  Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select one of the following versions:
  - 0 – *Spanning Tree Protocol* (STP)
  - 1 – Not supported
  - 2 – *Rapid Spanning tree Protocol* (RSTP)
  - 3 – *Multiple Spanning Tree Protocol* (MSTP). This is the default setting

- **guard root**

  Enables Root Guard for the port

  The Root Guard disables superior *Bridge Protocol Data Unit* (BPDU) reception. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state (root-inconsistent STP state). This state is equivalent to a listening state, and data is not forwarded across the port. Therefore, enabling the guard root enforces the root bridge position. Use the no parameter with this command to disable the Root Guard.

- **portfast**

  Enables rapid transitions. Enabling PortFast allows the port to bypass the listening and learning states.
- **spanning-tree** [bpdufilter|bpduguard] [default|disable|enable]

  **bpdufilter**
  [default|disable|enable]
  Sets a PortFast BPDU filter for the port
  Use the no parameter with this command to revert the port BPDU filter to its default.
  The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs.

  **bpduguard**
  [default|disable|enable]
  Enables BPDU guard on a port
  Use the no parameter with this command to set BPDU guard to its default.
  When the BPDU guard is set for a bridge, all PortFast-enabled ports that have the BPDU guard set to default shut down upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after a specified interval.

- **spanning-tree link-type** [point-to-point|shared]

  **link-type**
  [point-to-point|shared]
  Enables point-to-point or shared link types
  - point-to-point – Enables rapid transition. This option indicates the port should be treated as connected to a point-to-point link. A port connected to a controller is a point-to-point link.
  - shared – Disables rapid transition. This option indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link.

- **spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]

  **mst <0-15>**
  Configures MST on a spanning tree

  **cost <1-200000000>**
  Defines path cost for a port from 1 - 200000000. The default path cost depends on the speed of the port. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

  **port-priority <0-240>**
  Defines port priority for a bridge from 1 - 240. Lower the priority greater is the likelihood of the port becoming a designated port. Applying a higher value impacts the port’s likelihood of becoming a designated port.

- **spanning-tree port-cisco-interoperability** [disable|enable]

  **port-cisco-interoperability**
  Enables interoperability with Cisco’s version of MSTP (which is incompatible with standard MSTP)

  **enable**
  Enables CISCO Interoperability

  **disable**
  Disables CISCO Interoperability. The default is disabled.

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree bpdufilter disable
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree bpduguard enable
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree force-version 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree guard root
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree mst 2 port-priority 10
```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
interface ge1
description This is GigabitEthernet interface for Royal King
duplex full
spanning-tree bpduguard enable
spanning-tree bpdufilter disable
spanning-tree force-version 1
spanning-tree guard root
spanning-tree mst 2 port-priority 10
--More--
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes spanning tree settings configured on this interface</td>
</tr>
</tbody>
</table>
### 7.1.34.2.17 speed

**interface-config-instance**

Specifies the speed of a FastEthernet (10/100) or GigabitEthernet (10/100/1000) port. This is the speed at which the port can receive and transmit the data.

**Supported in the following platforms:**

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX  
- Wireless Controllers — RFS4000, RFS6000, RFS7000  
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
speed [10|100|1000|auto]
```

**Parameters**

- **speed [10|100|1000|auto]**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Forces 10 Mbps operation</td>
</tr>
<tr>
<td>100</td>
<td>Forces 100 Mbps operation</td>
</tr>
<tr>
<td>1000</td>
<td>Forces 1000 Mbps operation</td>
</tr>
<tr>
<td>auto</td>
<td>Port automatically detects its operational speed based on the port at the other end of the link. Select this option to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Set the interface speed to auto detect and use the fastest speed available. Speed detection is based on connected network hardware.

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#speed 10
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
interface ge1
  description This is GigabitEthernet interface for Royal King
  speed 10
  duplex full
  spanning-tree bpduguard enable
  spanning-tree bpdufilter disable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  dot1x supplicant username Bob password 0 test@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

**Related Commands**

- **no** Resets speed to default (auto)
7.1.34.2.18 switchport

Sets switching mode characteristics for the selected interface

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
switchport [access|mode|trunk]

switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

Parameters

- `switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]`
  - Sets the VLAN when interface is in the access mode. You can either directly specify the native VLAN ID or use a VLAN alias to identify the native VLAN.
  - `<1-4094>` – Specify the SVI VLAN ID from 1 - 4094.
  - `<VLAN-ALIAS-NAME>` – Specify the VLAN alias name (should be existing and configured).
  - An Ethernet port in the access mode accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN.

- `switchport mode [access|trunk]`
  - Sets the interface’s switching mode to access or trunk (can only be used on physical - layer 2 - interfaces)
  - `access` – If access mode is selected, the access VLAN is automatically set to VLAN1. In this mode, only untagged packets in the access VLAN (vlan1) are accepted on this port. All tagged packets are discarded.
  - `trunk` – If trunk mode is selected, tagged VLAN packets are accepted. The native VLAN is automatically set to VLAN1. Untagged packets are placed in the native VLAN by the wireless controller or service platform. Outgoing packets in the native VLAN are sent untagged. The default mode for both ports is trunk.
- switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]

<table>
<thead>
<tr>
<th>trunk allowed</th>
<th>Sets trunking mode, allowed VLANs characteristics of the port. Use this option to add VLANs that exclusively send packets over the listed port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan [&lt;VLAN-ID&gt;]</td>
<td>Sets allowed VLAN options. The options are:</td>
</tr>
<tr>
<td>add &lt;VLAN-ID&gt;</td>
<td>• &lt;VLAN-ID&gt; – Allows a group of VLAN IDs. Specify the VLAN IDs, can be either a range (55-60) or a comma-separated list (35, 41 etc.)</td>
</tr>
<tr>
<td>none</td>
<td>• none – Allows no VLANs to transmit or receive through the layer 2 interface</td>
</tr>
<tr>
<td>remove &lt;VLAN-ID&gt;</td>
<td>• add &lt;VLAN-ID&gt; – Adds VLANs to the current list</td>
</tr>
<tr>
<td></td>
<td>• &lt;VLAN-ID&gt; – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.)</td>
</tr>
<tr>
<td></td>
<td>• remove &lt;VLAN-ID&gt; – Removes VLANs from the current list</td>
</tr>
<tr>
<td></td>
<td>• &lt;VLAN-ID&gt; – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.)</td>
</tr>
</tbody>
</table>

**Note:** Allowed VLANs are configured only when the switching mode is set to “trunk”.

- switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]

<table>
<thead>
<tr>
<th>trunk</th>
<th>Sets trunking mode characteristics of the switchport</th>
</tr>
</thead>
<tbody>
<tr>
<td>native</td>
<td>Configures the native VLAN ID for the trunk-mode port</td>
</tr>
<tr>
<td></td>
<td>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.</td>
</tr>
<tr>
<td></td>
<td>• tagged – Tags the native VLAN. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header enabling upstream Ethernet devices to know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.</td>
</tr>
<tr>
<td></td>
<td>• vlan [&lt;1-4094&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify a value from 1 - 4094.</td>
</tr>
<tr>
<td></td>
<td>• &lt;VLAN-ALIAS-NAME&gt; – Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Interfaces ge1 - ge4 can be configured as trunk or in access mode. An interface configured as “trunk” allows packets (from the given list of VLANs) to be added to the trunk. An interface configured as “access” allows packets only from native VLANs.

Use the [no] switchport (access|mode|trunk) to undo switchport configurations.

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#switchport trunk native tagged
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#switchport access vlan 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
interface ge1
    description This is GigabitEthernet interface for Royal King
    speed 10
duplex full
    switchport mode access
    switchport access vlan 1
    spanning-tree bpduguard enable
    spanning-tree bpdufilter disable
    spanning-tree force-version 1
    spanning-tree guard root
    spanning-tree mst 2 port-priority 10
dot1x supplicant username Bob password 0 test@123
    ip dhcp trust
    ip arp header-mismatch-validation
    qos trust dscp
    qos trust 802.1p
    channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts interface settings to their default</td>
</tr>
</tbody>
</table>
7.34.2.19 use

interface-config-instance

Specifies the IP (IPv4 and IPv6) access list and MAC access list used with this Ethernet port. The associated ACL firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
use [ip-access-list in <IPv4-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]
```

Parameters

- use [ip-access-list in <IPv4-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-access-list in</td>
<td>Associates an IPv4 access list with this Ethernet port. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.</td>
</tr>
</tbody>
</table>
| <IPv4-ACCESS-LIST-NAME> | • in – Applies the IPv4 ACL on incoming packets  
|                        |   • <IPv4-ACCESS-LIST-NAME> – Specify the IPv4 access list name (it should be an existing and configured).                                      |
| ipv6-access-list in    | Associates an IPv6 access list with this Ethernet port. IPv6 is the latest revision of the IP designed to replace IPv4. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| <IPv6-ACCESS-LIST-NAME> | • in – Applies the IPv6 ACL on incoming packets  
|                        |   • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name (it should be an existing and configured).                                      |
| mac-access-list in     | Associates a MAC access list with this Ethernet port. MAC ACLs filter/mark packets based on the MAC address from which they arrive, as opposed to filtering packets on layer 2 ports. |
| <MAC-ACCESS-LIST-NAME> | • in – Applies the MAC ACL on incoming packets  
|                        |   • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name (it should be an existing and configured).                                      |

Examples

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#use mac-access-list in test
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#use ip-access-list in test
```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context interface ge1
description This is GigabitEthernet interface for Royal King
speed 10
duplex full
switchport mode access
switchport access vlan 1
use ip-access-list in test
use mac-access-list in test
spanning-tree bpduguard enable
spanning-tree bpdufilter disable
spanning-tree force-version 1
--More--
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disassociates the IP access list or MAC access list from the interface</td>
</tr>
</tbody>
</table>
7.1.34.3 interface-config-vlan-instance

Use the config-profile-<DEVICE-PROFILE-NAME> mode to configure Ethernet, VLAN and tunnel settings.

To switch to this mode, use the following commands:

```
<DEVICE>(config-profile-default-<DEVICE-TYPE>)#interface [<INTERFACE-NAME>|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]| up1|vlan <1-4094>|wwan1|xge <1-24>]
```

The following example uses the config-profile-default-rfs7000 instance to configure a VLAN interface:

```
rfs7000-37FABE(config-profile-default-rfs7000)#interface vlan 8
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

The following table summarizes interface VLAN configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>Defines the encryption module used with this VLAN interface</td>
<td>page 7-201</td>
</tr>
<tr>
<td>description</td>
<td>Defines the VLAN interface description</td>
<td>page 7-202</td>
</tr>
<tr>
<td>dhcp</td>
<td>Enables inclusion of optional fields (client identifier) in DHCP client requests</td>
<td>page 7-203</td>
</tr>
<tr>
<td>dhcp-relay-incoming</td>
<td>Allows an onboard DHCP server to respond to relayed DHCP packets on this interface</td>
<td>page 7-204</td>
</tr>
<tr>
<td>ip</td>
<td>Configures the VLAN interface’s IP settings</td>
<td>page 7-205</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures the VLAN interface’s IPv6 settings</td>
<td>page 7-208</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts this VLAN interface’s settings to default</td>
<td>page 7-213</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down this VLAN interface</td>
<td>page 7-215</td>
</tr>
<tr>
<td>use</td>
<td>Associates an IP (IPv4 and IPv6) access list, bonjour-gw-discovery policy, and an IPv6-route-advertisement policy with this VLAN interface</td>
<td>page 7-216</td>
</tr>
</tbody>
</table>
7.1.34.3.1 crypto

interface-config-vlan-instance

Associates an existing and configured VPN crypto map with this VLAN interface. Crypto map entries are sets of configuration parameters for encrypting packets that pass through the VPN tunnel. For more information on crypto maps, see crypto-map-config-commands.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
crypto map <CRYPTO-MAP-NAME>

Parameters
- crypto map <CRYPTO-MAP-NAME>

Examples
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#crypto map map1
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
  interface vlan8
  crypto map map1
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

Related Commands
- no
  Disables or reverts interface VLAN settings to their default
7.1.34.3.2 description

interface-config-vlan-instance

Defines this VLAN interface’s description. Use this command to provide additional information about the VLAN.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

description <WORD>

Parameters
- description <WORD>

Examples

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#description “This VLAN interface is configured for the Sales Team”

testconf(config-profile-default-rfs7000-if-vlan8)#show context

- description This VLAN interface is configured for the Sales Team

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

Related Commands

no

Removes the VLAN interface description
7.1.34.3.3 dhcp

Enables inclusion of optional fields (client identifier) in DHCP client requests. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp client include client-identifier

Parameters

- dhcp client include client-identifier

| dhcp client include client-identifier | Enables inclusion of client identifier in DHCP client requests |

Examples

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#dhcp client include client-identifier

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
  interface vlan8
  dhcp client include client-identifier
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

Related Commands

- no | Disables inclusion of client identifier in DHCP client requests |
7.1.34.3.4 dhcp-relay-incoming

This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-relay-incoming

Parameters
None

Examples

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#dhcp-relay-incoming

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context interface vlan8
description This VLAN interface is configured for the Sales Team
crypto map map1
dhcp-relay-incoming

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts interface VLAN settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.3.5 ip

`interface-config-vlan-instance`

Configures the VLAN interface’s IP settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ip [address|dhcp|helper-address|nat|ospf]
ip helper-address <IP>
ip address [<IP/M>|<NETWORK-ALIAS-NAME>|dhcp|zeroconf] {secondary}
ip address dhcp
ip dhcp client request options all
ip nat [inside|outside]
ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|priority]
ip ospf authentication [message-digest|null|simple-password]
ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]
ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]
ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]
```

**Parameters**

- **ip helper-address <IP>**
  - Enables DHCP and BOOTP requests forwarding for a set of clients. Configure a helper address on the VLAN interface connected to the client. The helper address should specify the address of the BOOTP or DHCP servers to receive the requests. If you have multiple servers, configure one helper address for each server.
  - `<IP>` – Specify the IP address of the DHCP or BOOTP server.

- **ip address [<IP/M>|<NETWORK-ALIAS-NAME>|zeroconf] {secondary}**
  - Sets the VLAN interface’s IP address
  - `<IP/M>` – Specifies the interface IP address in the A.B.C.D/M format
  - secondary – Optional. Sets the specified IP address as a secondary address
### Profiles 7-205

| `<NETWORK-ALIAS-NAME>` | Uses a pre-defined network alias to provide this VLAN interface’s IP address. Specify the network alias name.  
| | • secondary – Optional. Sets the network-alias provided IP address as the secondary address |
| `zeroconf {secondary}` | Uses Zero Configuration Networking (zeroconf) to generate an IP address for this interface  
| | Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device.  
| | • secondary – Optional. Sets the generated IP address as a secondary address |
| | | **ip address dhcp**  
| | address | Sets the VLAN interface’s IP address |
| | dhcp | Uses a DHCP client to obtain an IP address for this VLAN interface |
| | | **ip dhcp client request options all**  
| | dhcp | Uses a DHCP client to configure a request on this VLAN interface |
| | client | Configures a DHCP client |
| | request | Configures DHCP client request |
| | options | Configures DHCP client request options |
| | all | Configures all DHCP client request options |
| | | **ip nat [inside|outside]**  
| | nat [inside|outside] | Defines NAT settings for the VLAN interface. NAT is disabled by default.  
| | | • inside – Enables NAT on the inside interface. The inside network is transmitting data over the network to the intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.  
| | | • outside – Enables NAT on the outside interface. Packets passing through the NAT on the way back to the managed LAN are searched against the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network. |
| | | **ip ospf authentication [message-digest|null|simple-password]**  
| | ospf authentication | Configures OSPF authentication scheme. Options are message-digest, null, and simple-password. |
| | message-digest | Configures md5 based authentication |
| | null | No authentication required |
| | simple-password | Configures simple password based authentication |
- `ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]`

<table>
<thead>
<tr>
<th>ospf authentication-key</th>
<th>Configures an OSPF authentication key</th>
</tr>
</thead>
</table>
  | simple-password [0 <WORD>|2 <WORD>] | Configures a simple password OSPF authentication key
  | | - 0 <WORD> – Configures clear text key
  | | - 2 <WORD> – Configures encrypted key

- `ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]`

  | bandwidth <1-10000000> | Configures bandwidth for the physical port mapped to this layer 3 interface
  | | - <1-10000000> – Specify the bandwidth from 1 - 10000000.
  | cost <1-65535> | Configures OSPF cost
  | | - <1-65535> – Specify OSPF cost value from 1 - 65535.
  | priority <0-255> | Configures OSPF priority
  | | - <0-255> – Specify OSPF priority value from 0 - 255.

- `ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]`

  | ospf message-digest | Configures message digest authentication parameters |
  | key-id <1-255> | Configures message digest authentication key ID from 0 - 255 |
  | md5 [0 <WORD>|2 <WORD>] | Configures md5 key
  | | - 0 <WORD> – Configures clear text key
  | | - 2 <WORD> – Configures encrypted key

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip address 10.0.0.1/8
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip nat inside
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip helper-address 172.16.10.3
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#ip dhcp client request options all
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context interface vlan8
description This VLAN interface is configured for the Sales Team
ip address 10.0.0.1/8
ip dhcp client request options all
ip helper-address 172.16.10.3
ip nat inside
crypto map map1
dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

**Related Commands**

`no` | Removes or resets IP settings on this interface
7.1.34.3.6 ipv6

Configure the VLAN interface’s IPv6 settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ipv6 [accept|address|dhcp|enable|enforce-dad|mtu|redirects|request-dhcpv6-options|router-advertisements]

ipv6 accept ra {<no-default-router|no-hop-limit|no-mtu>}

ipv6 address [<IPv6/M>|autoconfig|eui-64|link-local|prefix-from-provider]

ipv6 address [<IPv6/M]|autoconfig]
ipv6 address eui-64 [<IPv6/M>|prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>]
ipv6 address prefix-from-provider <WORD> <HOST-PORTION/LENGTH>
ipv6 address link-local <LINK-LOCAL-ADD>

ipv6 dhcp [client [information|prefix-from-provider <WORD>]|relay destination <DEST-IPv6-ADD>]

ipv6 [enable|enforce-dad|mtu <1280-1500>|redirects|request-dhcpv6-options]

ipv6 router-advertisements [prefix <IPv6-PREFIX>|prefix-from-provider <WORD>]
{<no-autoconfig|off-link|site-prefix|valid-lifetime}
### ipv6 address [<IPv6/M>|autoconfig]

**ipv6 address**
**[<IPv6/M>|autoconfig]**

Configures IPv6 address related settings on this VLAN interface.

- **<IPv6>** – Specify the non-link local static IPv6 address and prefix length of the interface in the X:X::X:X/M format.
- **autoconfig** – Enables stateless auto-configuration of IPv6 address, based on the prefixes received from RAs (with auto-config flag set). These prefixes are used to auto-configure the IPv6 address. This option is enabled by default. Use the `no > ipv6 > address > autoconfig` command to negate the use of prefixes received in RAs.

### ipv6 address eui-64 [<IPv6/M>|prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>]

**ipv6 address eui-64**

Configures the IPv6 prefix and prefix length. This prefix is used to auto-generate the static IPv6 address (for this interface) in the modified Extended Unique Identifier (EUI)-64 format.

Implementing the IEEE's 64-bit EUI64 format enables a host to automatically assign itself a unique 64-bit IPv6 interface identifier, without manual configuration or DHCP. This is accomplished on a virtual interface by referencing the already unique 48-bit MAC address, and reformatting it to match the EUI-64 specification.

#### Note:
In the EUI-64 IPv6 address the prefix and host portions are each 64 bits in length.

**<IPv6/M>**

Specify the IPv6 prefix and prefix length. This configured value is used as the prefix portion of the auto-generated IPv6 address, and the host portion is derived from the MAC address of the interface.

**Note:** Any bits of the configured value exceeding the prefix-length "M" are ignored and replaced by the host portion derived from the MAC address.

For example:
Prefix portion provided using this command: `ipv6 > address > eui-64 > 2004:b055:15:dead::1111/64`.
Host portion derived using the interface's MAC address (00-15-70-37-FB-5E): 215:70ff:fe37:fb5e

In this example, the host part ":1111" is ignored and replaced with the modified eui-64 formatted host address.

**prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>**

Configures the “prefix-from-provider” named object and the associated IPv6 prefix and prefix length. This configured value is used as the prefix portion of the auto-generated IPv6 address, and the host portion is derived from the MAC address of the interface.

- **<WORD>** – Specify the IPv6 “prefix-from-provider” object’s name. This is the IPv6 general prefix (32 character maximum) name provided by the internet service provider.
- **<IPv6-PREFIX/PREFIX-LENGTH>** – Specify the IPv6 address subnet and host parts along with prefix length (site-renumbering).

For example:
Prefix portion provided using this command: `ipv6 > address > eui-64 > prefix-from-provider > ISP1-prefix > 2002::/64`.
Host portion derived using the interface’s MAC address (00-15-70-37-FB-5E): 215:70ff:fe37:fb5e
Auto-configured IPv6 address using the above prefix and host portions: `2002::215:70ff:fe37:fb5e/64`
• `ipv6 address prefix-from-provider <WORD> <HOST-PORTION/LENGTH>`

<table>
<thead>
<tr>
<th>ipv6 address</th>
<th>Configures the IPv6 address related settings on this VLAN interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-from-provider <code>&lt;WORD&gt;</code> <code>&lt;HOST-PORTION/LENGTH&gt;</code></td>
<td>Configures the “prefix-from-provider” named object and the host portion of the IPv6 interface address. The prefix derived from the specified “prefix-from-provider” and the host portion (second parameter) are combined together (using the prefix-length of the specified “prefix-from-provider”) to generate the interface’s IPv6 address.</td>
</tr>
<tr>
<td>– <code>&lt;WORD&gt;</code> – Provide the “prefix-from-provider” object’s name. This is the IPv6 general prefix (32 character maximum) name provided by the service provider.</td>
<td></td>
</tr>
<tr>
<td>– <code>&lt;HOST-PORTION/LENGTH&gt;</code> – Provide the subnet number, host portion, and prefix length used to form the actual address along with the prefix derived from the “prefix-from-provider” object identified by the <code>&lt;WORD&gt;</code> keyword.</td>
<td></td>
</tr>
</tbody>
</table>

• `ipv6 address link-local <LINK-LOCAL-ADD>`

<table>
<thead>
<tr>
<th>ipv6 address</th>
<th>Configures the IPv6 address related settings on this VLAN interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-local <code>&lt;LINK-LOCAL-ADD&gt;</code></td>
<td>Configures IPv6 link-local address on this interface. The configured value overrides the default link-local address derived from the interface’s MAC address. Use the <code>no ipv6 link-local</code> command to restore the default link-local address derived from MAC address.</td>
</tr>
<tr>
<td>Note: It is mandatory for an IPv6 interface to always have a link-local address.</td>
<td></td>
</tr>
</tbody>
</table>

• `ipv6 dhcp [client [information|prefix-from-provider <WORD>]] relay destination <DEST-IPv6-ADD>`

<table>
<thead>
<tr>
<th>ipv6 dhcp [client [information] [prefix-from-provider &lt;WORD&gt;]]</th>
<th>Configures DHCPv6 client-related settings on this VLAN interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>– information – Configures stateless DHCPv6 client on this interface. When enabled, the device can request configuration information from the DHCPv6 server using stateless DHCPv6. This option is disabled by default.</td>
<td></td>
</tr>
<tr>
<td>– prefix-from-provider – Configures prefix-delegation client on this interface. Enter the IPv6 general prefix (32 character maximum) name provided by the service provider.</td>
<td></td>
</tr>
<tr>
<td>– destination – Forwards DHCPv6 packets to a specified DHCPv6 relay</td>
<td></td>
</tr>
<tr>
<td>– <code>&lt;DEST-IPv6-ADD&gt;</code> – Specify the destination DHCPv6 relay’s address.</td>
<td></td>
</tr>
<tr>
<td>Note: DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When a DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.</td>
<td></td>
</tr>
</tbody>
</table>

• `ipv6 [enable|enforce-dad|mtu <1280-1500>|redirects|request-dhcp-options]`

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Configures IPv6 settings on this VLAN interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables IPv6 on this interface. This option is disabled by default.</td>
</tr>
<tr>
<td>enforce-dad</td>
<td>Enforces <em>Duplicate Address Detection</em> (DAD) on wired ports. This option is enabled by default.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mtu &lt;1280-1500&gt;</td>
<td>Configures the Maximum Transmission Unit (MTU) for IPv6 packets on this interface.</td>
</tr>
<tr>
<td>redirects</td>
<td>Enables ICMPv6 redirect messages sending on this interface. This option is enabled by default.</td>
</tr>
<tr>
<td>request-dhcp-options</td>
<td>Requests options from DHCPv6 server on this interface. This option is disabled by default.</td>
</tr>
</tbody>
</table>

- ipv6 router-advertisements [prefix <IPv6-PREFIX>|prefix-from-provider <WORD>] {no-autoconfig|off-link|site-prefix <SITE-PREFIX>|valid-lifetime}

- Configures IPv6 RA related settings on this VLAN interface.
- Configures a static prefix and its related parameters. The configured value is advertised on RAs. 
  - <IPv6-PREFIX> – Specify the IPv6 prefix.
- Configures a static "prefix-from-provider" named object and its related parameters on this VLAN interface. The configured value is advertised on RAs. 
  - <WORD> – Specify the "prefix-from-provider" named object’s name.
- This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords.
  - no-autoconfig – Optional. Disables the setting of the auto configuration flag in the prefix. When configured, the configured prefixes are not used for IPv6 address generation. The autoconfiguration option is enabled by default. Using no-autoconfig disables it.
- This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords.
  - off-link – Optional. Disables the setting of the on-link flag in the prefix. The on-link option is enabled by default. Using off-link disables it.
- This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords.
  - site-prefix <SITE-PREFIX> – Configures subnet (site) prefix
- This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords.
  - valid-lifetime – Configures the valid lifetime for the prefix
  - preferred-lifetime – Configures preferred lifetime for the prefix
  - &lt;30-4294967294&gt; – Configures the valid/preferred lifetime in seconds
  - at – Configures expiry time and date of the valid/preferred lifetime
  - infinite – Configures the valid/preferred lifetime as infinite
Examples

rfs7000-6DCD4B(config-profile-test-if-vlan4)#ipv6 enable

rfs7000-6DCD4B(config-profile-test-if-vlan4)#ipv6 accept ra no-mtu

rfs7000-6DCD4B(config-profile-test-if-vlan4)#ipv6 address eui-64 prefix-from-provider ISP1-prefix 2002::/64

rfs7000-6DCD4B(config-profile-test-if-vlan4)#show context
interface vlan4
  ipv6 enable
  ipv6 address eui-64 prefix-from-provider ISP1-prefix 2002::/64
  ipv6 accept ra no-mtu

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes or resets IPv6 settings on this VLAN interface</td>
</tr>
</tbody>
</table>
7.1.34.3.7 no

Negates a command or reverts to defaults. The no command, when used in the Config Interface VLAN mode, negates VLAN interface settings or reverts them to their default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
no [crypto|description|dhcp|dhcp-relay-incoming|ip|ipv6|shutdown|use]
no dhcp client include client-identifier
no [crypto map|description|dhcp-relay-incoming|shutdown]
no ip [address|dhcp|helper-address|nat|ospf]
no ip [helper-address <IP>|nat]
no ip address {<IP/M> |secondary|<NETWORK-ALIAS-NAME> |secondary|dhcp|
zeroconf |secondary}
no ip dhcp client request options all
no ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|
priority]
no ipv6 [accept|address|dhcp|enable|enforce-dad|mtu|redirects|request-dhcpv6-options|
router-advertisement]
no ipv6 [accept ra|enable|enforce-dad|mtu|redirects|request-dhcpv6-options]
no ipv6 address [{<IPv6/M>|autoconfig|eui-64|link-local|prefix-from-provider>}
no ipv6 dhcp [client|relay]
no ipv6 router-advertisement [prefix <WORD>|prefix-from-provider <WORD>]
no use [bonjour-gw-discovery-policy]|ip-access-list in|ipv6-access-list in|
ipv6-router-advertisement-policy|url-filter]
```

Parameters

- no <PARAMETERS>

Examples

The following example shows the VLAN interface settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
interface vlan8
    description This VLAN interface is configured for the Sales Team
    ip address 10.0.0.1/8
    ip dhcp client request options all
    ip nat inside
    crypto map map1
dhcp-relay-incoming
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no crypto map
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no description
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#no ip dhcp client request options all
```
The following example shows the VLAN interface settings after the 'no' commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
interface vlan8
  ip address 10.0.0.1/8
  ip helper-address 172.16.10.3
  ip nat inside
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#

7.1.34.3.8 shutdown

*interface-config-vlan-instance*

Shuts down the selected interface. Use the no shutdown command to enable an interface.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`shutdown`

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#shutdown
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context interface vlan8
  ip address 10.0.0.1/8
  ip helper-address 172.16.10.3
  shutdown
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts interface VLAN settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.3.9 use

`interface-config-vlan-instance`

Associates an IP (IPv4 and IPv6) access list, bonjour-gw-discovery policy, and an IPv6-router-advertisement policy with this VLAN interface.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use [bonjour-gw-discovery-policy <POLICY-NAME> | ip-access-list in <IP-ACL-NAME> | ipv6-access-list in <IPv6-ACL-NAME> | ipv6-router-advertisement-policy <POLICY-NAME> | url-filter <URL-FILTER-NAME>]
```

**Parameters**

- `use [bonjour-gw-discovery-policy <POLICY-NAME> | ip-access-list in <IP-ACL-NAME> | ipv6-access-list in <IPv6-ACL-NAME> | ipv6-router-advertisement-policy <POLICY-NAME> | url-filter <URL-FILTER-NAME>]

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| bonjour-gw-discovery-policy <POLICY-NAME> | Uses an existing Bonjour GW Discovery policy with this VLAN interface. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming over the VLAN interface.  
  - `<POLICY-NAME>` – Specify the Bonjour GW Discovery policy name (should be existing and configured).  
  Note: For more information on Bonjour GW Discovery policy, see `bonjour-gw-discovery-policy`. |
| ip-access-list in <IP-ACCESS-LIST-NAME> | Uses a specified IPv4 access list with this interface  
  - `in` – Applies IPv4 ACL to incoming packets  
  - `<IP-ACCESS-LIST-NAME>` – Specify the IPv4 access list name. |
| ipv6-access-list in <IPv6-ACCESS-LIST-NAME> | Uses a specified IPv6 access list with this interface  
  - `in` – Applies IPv6 ACL to incoming packets  
  - `<IPv6-ACCESS-LIST-NAME>` – Specify the IPv6 access list name. |
| ipv6-router-advertisement-policy <POLICY-NAME> | Uses an existing IPv6 router advertisement policy with this VLAN interface.  
  - `<POLICY-NAME>` – Specify the IPv6 router advertisement policy name (should be existing and configured). |
| url-filter <URL-FILTER-NAME> | Enforces URL filtering on this VLAN interface by associating a URL filter  
  - `<URL-FILTER-NAME>` – Specify the URL filter name (should be existing and configured). |

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#use ip-access-list in test
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#show context
  interface vlan8
    ip address 10.0.0.1/8
    use ip-access-list in test
      ip helper-address 172.16.10.3
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts interface VLAN settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.4 interface-config-radio-instance

This section documents radio interface configuration parameters applicable only to the access point profiles and the RFS4011 profile.

The access point radio interface can be radio1, radio2, or radio3. Legacy AP71XX models contain either a single or a dual radio configuration. Newer AP71XXN model access points support single, dual, or triple radio configurations. An AP650 model access point is available in either single or dual radio models. The remainder of the access point portfolio are dual-radio models.

To enter the AP/RFS4000 profile > radio interface context, use the following commands:

```
<DEVICE>(config)#profile RFS4000 <RFS4000-PROFILE-NAME>
<DEVICE>(config)#profile <AP-TYPE> <PROFILE-NAME>
```

```
rfs7000-37FABE(config)#profile ap71xx 71xxTestProfile
rfs7000-37FABE(config-profile-71xxTestProfile)#
```

```
rfs7000-37FABE(config-profile-71xxTestProfile)#interface radio 1
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#? 
```

Radio Mode commands:

- **adaptivity**
- **aeroscout**
- **aggregation**
- **airtime-fairness**
- **antenna-diversity**
- **antenna-downtilt**
- **antenna-elevation**
- **antenna-gain**
- **antenna-mode**
- **assoc-response**
- **association-list**
- **beacon**
- **bridge**
- **channel**
- **data-rates**
- **description**
- **dfs-rehome**
- **dynamic-chain-selection**
- **ekahau**
- **extended-range**
- **fallback-channel**
- **guard-interval**
- **ldpc**
- **lock-rf-mode**
- **max-clients**
- **mesh**
- **meshpoint**
- **no**
- **non-unicast**
- **off-channel-scan**
- **placement**

Adaptivity
Aeroscout Multicast MAC/Enable
Configure 802.11n aggregation related parameters
Enable fair access to medium for clients based on their usage of airtime
Transmit antenna diversity for non-11n transmit rates
Enable ADEPT antenna mode
Specifies the antenna elevation gain
Specifies the antenna gain of this radio
Configure the antenna mode (number of transmit and receive antennas) on the radio
Configure transmission parameters for Association Response frames
Configure the association list for the radio
Configure beacon parameters
Configure rf-mode related configuration
Configure the channel of operation for this radio
Specify the 802.11 rates to be supported on this radio
Configure a description for this radio
Revert to configured home channel once dfs evacuation period expires
Automatic antenna-mode selection (single antenna for non-11n transmit rates)
Ekahau Multicast MAC/Enable
Configure extended range
Configure the channel to be used for falling back in the event of radar being detected on the current operating channel
Configure the 802.11n guard interval
Configure support for Low Density Parity Check Code
Retain user configured rf-mode setting for this radio
Maximum number of wireless clients allowed to associate subject to AP limit
Configure radio mesh parameters
Enable meshpoints on this radio
Negate a command or set its defaults
Configure handling of non-unicast frames
Enable off-channel scanning on the radio
Configure the location where this radio is
power operating Configure the transmit power of the radio
preamble-short Use short preambles on this radio
probe-response Configure transmission parameters for Probe Response frames
radio-resource-measurement Configure support for 802.11k Radio Resource Measurement
radio-share-mode Configure the radio-share mode of operation for this radio
rate-selection Default or Opportunistic rate selection
remove-override Negate a command or set its defaults
rf-mode Configure the rf-mode of operation for this radio
rifs Configure Reduced Interframe Spacing (RIFS) parameters
rts-threshold Configure the RTS threshold
shutdown Shutdown the selected radio interface
smart-rf Configure radio specific smart-rf settings
sniffer-redirect Capture packets and redirect to an IP address running a packet capture/analysis tool
stbc Configure Space-Time Block Coding (STBC) parameters
transmit-beamforming Enable Transmit Beamforming
use Set setting to use
wips Wireless intrusion prevention related configuration
wireless-client Configure wireless client related parameters
wlan Enable wlans on this radio
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

The following table summarizes the radio interface configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>adaptivity</td>
<td>Configures an adaptivity timeout value, in minutes, for avoidance of channels detected with radar or high levels of interference</td>
<td>page 7-222</td>
</tr>
<tr>
<td>aeroscout</td>
<td>Enables Aeroscout multicast packet forwarding</td>
<td>page 7-223</td>
</tr>
<tr>
<td>aggregation</td>
<td>Configures 802.11n aggregation parameters</td>
<td>page 7-224</td>
</tr>
<tr>
<td>airtime-fairness</td>
<td>Enables fair access for clients based on airtime usage</td>
<td>page 7-227</td>
</tr>
<tr>
<td>antenna-diversity</td>
<td>Transmits antenna diversity for non-11n transmit rates</td>
<td>page 7-228</td>
</tr>
<tr>
<td>antenna-downtilt</td>
<td>Enables Advanced Element Panel Technology (ADEPT) antenna mode</td>
<td>page 7-229</td>
</tr>
<tr>
<td>antenna-elevation</td>
<td>Configures the antenna’s elevation gain. This command is applicable only to the AP7562 model access point</td>
<td>page 7-230</td>
</tr>
<tr>
<td>antenna-gain</td>
<td>Specifies the antenna gain for the selected radio</td>
<td>page 7-232</td>
</tr>
<tr>
<td>antenna-mode</td>
<td>Configures the radio antenna mode</td>
<td>page 7-233</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>assoc-response</td>
<td>Enables an access point to ignore or respond to an association/authorization request based on the configured Received Signal Strength Index (RSSI) threshold and deny-threshold values</td>
<td>page 7-234</td>
</tr>
<tr>
<td>association-list</td>
<td>Associates an existing global association list with this radio interface</td>
<td>page 7-235</td>
</tr>
<tr>
<td>beacon</td>
<td>Configures beacon parameters</td>
<td>page 7-236</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures client-bridge related parameters, if the selected radio is functioning as a client bridge. This option is applicable only on radio 2 of the AP6522 and AP6562 model access points.</td>
<td>page 7-238</td>
</tr>
<tr>
<td>channel</td>
<td>Configures a radio’s channel of operation</td>
<td>page 7-248</td>
</tr>
<tr>
<td>data-rates</td>
<td>Specifies the 802.11 rates supported on a radio</td>
<td>page 7-249</td>
</tr>
<tr>
<td>description</td>
<td>Configures the selected radio’s description</td>
<td>page 7-253</td>
</tr>
<tr>
<td>dfs-rehome</td>
<td>Reverts to configured home channel once Dynamic Frequency Selection (DFS) evacuation period expires</td>
<td>page 7-254</td>
</tr>
<tr>
<td>dynamic-chain-selection</td>
<td>Enables automatic antenna mode selection</td>
<td>page 7-255</td>
</tr>
<tr>
<td>ekahau</td>
<td>Enables Ekahau multicast packet forwarding</td>
<td>page 7-256</td>
</tr>
<tr>
<td>extended-range</td>
<td>Configures extended range</td>
<td>page 7-257</td>
</tr>
<tr>
<td>fallback-channel</td>
<td>Configures the channel to which the radio switches in case of radar detection on the current channel</td>
<td>page 7-258</td>
</tr>
<tr>
<td>guard-interval</td>
<td>Configures the 802.11n guard interval</td>
<td>page 7-259</td>
</tr>
<tr>
<td>ldpc</td>
<td>Enables support for Low Density Parity Check (LDPC) on the radio interface</td>
<td>page 7-260</td>
</tr>
<tr>
<td>lock-rf-mode</td>
<td>Retains user configured RF mode settings for the selected radio</td>
<td>page 7-261</td>
</tr>
<tr>
<td>max-clients</td>
<td>Configures the maximum number of wireless clients allowed to associate with this radio</td>
<td>page 7-262</td>
</tr>
<tr>
<td>mesh</td>
<td>Configures radio mesh parameters</td>
<td>page 7-263</td>
</tr>
<tr>
<td>meshpoint</td>
<td>Maps an existing meshpoint to this radio interface</td>
<td>page 7-265</td>
</tr>
<tr>
<td>no</td>
<td>Negates or resets radio interface settings configures on a profile or a device</td>
<td>page 7-266</td>
</tr>
<tr>
<td>non-unicast</td>
<td>Configures the handling of non unicast frames on this radio</td>
<td>page 7-269</td>
</tr>
<tr>
<td>off-channel-scan</td>
<td>Enables selected radio’s off channel scanning parameters</td>
<td>page 7-271</td>
</tr>
<tr>
<td>placement</td>
<td>Defines selected radio’s deployment location</td>
<td>page 7-273</td>
</tr>
<tr>
<td>power</td>
<td>Configures the transmit power on this radio</td>
<td>page 7-274</td>
</tr>
<tr>
<td>preamble-short</td>
<td>Enables the use of short preamble on this radio</td>
<td>page 7-275</td>
</tr>
<tr>
<td>probe-response</td>
<td>Configures transmission parameters for probe response frames</td>
<td>page 7-276</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>radio-resource-</td>
<td>Enables 802.11k radio resource measurement</td>
<td>page 7-277</td>
</tr>
<tr>
<td>measurement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radio-share-mode</td>
<td>Configures the mode of operation, for this radio, as radio-share</td>
<td>page 7-278</td>
</tr>
<tr>
<td>rate-selection</td>
<td>Sets the rate selection method to standard or opportunistic</td>
<td>page 7-279</td>
</tr>
<tr>
<td>rf-mode</td>
<td>Configures the radio’s RF mode</td>
<td>page 7-280</td>
</tr>
<tr>
<td>rifs</td>
<td>Configures Reduced Interframe Spacing (RIFS) parameters on this radio</td>
<td>page 7-282</td>
</tr>
<tr>
<td>rts-threshold</td>
<td>Configures the Request to Send (RTS) threshold value on this radio</td>
<td>page 7-283</td>
</tr>
<tr>
<td>service</td>
<td>Enables dynamic control function. This dynamic function controls performance of the radio receiver’s low noise amplifiers (LNAs).</td>
<td>page 7-285</td>
</tr>
<tr>
<td>shutdown</td>
<td>Terminates or shuts down selected radio interface</td>
<td>page 7-286</td>
</tr>
<tr>
<td>smart-rf</td>
<td>Overrides Smart RF channel width setting on the selected radio interface</td>
<td>page 7-287</td>
</tr>
<tr>
<td>sniffer-redirect</td>
<td>Captures and redirects packets to an IP address running a packet capture/analysis tool</td>
<td>page 7-288</td>
</tr>
<tr>
<td>stbc</td>
<td>Configures radio’s Space Time Block Coding (STBC) mode</td>
<td>page 7-290</td>
</tr>
<tr>
<td>transmit-beamforming</td>
<td>Enables transmit beamforming on the selected radio interface</td>
<td>page 7-291</td>
</tr>
<tr>
<td>use</td>
<td>Enables use of an association ACL policy and a radio QoS policy by selected radio interface</td>
<td>page 7-292</td>
</tr>
<tr>
<td>wips</td>
<td>Enables access point to change its channel of operation in order to terminate rogue devices</td>
<td>page 7-294</td>
</tr>
<tr>
<td>wireless-client</td>
<td>Configures wireless client parameters on selected radio</td>
<td>page 7-295</td>
</tr>
<tr>
<td>wlan</td>
<td>Enables a WLAN on selected radio</td>
<td>page 7-296</td>
</tr>
</tbody>
</table>
### 7.1.34.1 adaptivity

Configure an interval, in minutes, for avoiding channels detected with high levels of interference.

As per the *European Telecommunications Standards Institute* (ETSI) EN 300 328 V1.8.1/ ETSI EN 301 893 V1.7.1 requirements, access points have to monitor interference levels on operating channels, and stop functioning on channels with interference levels exceeding ETSI-specified threshold values.

This command configures the interval for which a channel is avoided on detection of interference, and is applicable only if the channel selection mode is set to ACS, Random, or Fixed.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Parameter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adaptivity [recovery</td>
<td>timeout &lt;30-3600&gt;]</td>
</tr>
<tr>
<td>recovery</td>
<td>Enables switching of channels when an access point’s radio is in the adaptivity mode. In the adaptivity mode, an access point monitors interference on its set channel and stops functioning when the radio’s defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default.</td>
</tr>
<tr>
<td>timeout &lt;30-3600&gt;</td>
<td>Configures an adaptivity timeout.</td>
</tr>
</tbody>
</table>

#### Examples

```
nx4500-5CFA2B(config-profile-testAP7532-if-radio1)#adaptivity timeout 200
```

```
nx4500-5CFA2B(config-profile-testAP7532-if-radio1)#show context interface radio1 adaptivity timeout 200
```

#### Related Commands

- `no` Removes the configured adaptivity timeout value and disables adaptivity recovery.
7.1.34.4.2 aeroscout

interface-config-radio-instance

Enables Aeroscout multicast packet forwarding. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

aeroscout [forward|mac <MAC>]

Parameters

- aeroscout [forward|mac <MAC>]

<table>
<thead>
<tr>
<th>aeroscout</th>
<th>Configures aeroscout enabling forwarding parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward</td>
<td>Enables Aeroscout multicast packet forwarding to a specified MAC address. When enabled, Aeroscout tags associate with an access point, then communicate with a location engine.</td>
</tr>
<tr>
<td>mac &lt;MAC&gt;</td>
<td>Configures the multicast MAC address to forward the packets</td>
</tr>
<tr>
<td></td>
<td>• &lt;MAC&gt; – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#aeroscout forward
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context interface radiol
  aeroscout forward
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

no | Disables Aeroscout Multicast packet forwarding
7.1.34.4.3 aggregation

Configures 802.11n frame aggregation parameters. Frame aggregation increases throughput by sending two or more data frames in a single transmission. There are two types of frame aggregation: *MAC Service Data Unit* (MSDU) aggregation and *MAC Protocol Data Unit* (MPDU) aggregation. Both modes group several data frames into one large data frame.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
aggregation [ampdu|amsdu]
aggregation ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing]
aggregation ampdu [rx-only|tx-only|tx-rx|none]
aggregation ampdu max-aggr-size [rx|tx]
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]
aggregation ampdu max-aggr-size tx <2000-65535>
aggregation ampdu min-spacing [0|1|2|4|8|16]
aggregation amsdu [rx-only|tx-rx]
```

**Parameters**

- **aggregation ampdu [rx-only|tx-only|tx-rx|none]**
  - *aggregation***: Configures 802.11n frame aggregation parameters
  - *ampdu***: Configures *Aggregate MAC Protocol Data Unit* (AMPDU) frame aggregation parameters. AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
  - *tx-only***: Supports the transmission of AMPDU aggregated frames only
  - *rx-only***: Supports the receipt of AMPDU aggregated frames only
  - *tx-rx***: Supports the transmission and receipt of AMPDU aggregated frames (default setting)
  - *none***: Disables support for AMPDU aggregation

- **aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]**
  - *aggregation***: Configures 802.11n frame aggregation parameters
  - *ampdu***: Configures AMPDU frame aggregation parameters. AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
### aggregation ampdu max-aggr-size tx <2000-65535>

**max-aggr-size**

Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.

**rx [8191|16383|32767|65535]**

Configures the maximum limit (in bytes) advertised for received frames

- 8191 – Advertises a maximum of 8191 bytes
- 16383 – Advertises a maximum of 16383 bytes
- 32767 – Advertises a maximum of 32767 bytes
- 65535 – Advertises a maximum of 65535 bytes (default setting)

### aggregation ampdu min-spacing [0|1|2|4|8|16|auto]

**min-spacing [0|1|2|4|8|16]**

Configures the minimum gap, in microseconds, between AMPDU frames

- 0 – Configures the minimum gap as 0 microseconds
- 1 – Configures the minimum gap as 1 microseconds
- 2 – Configures the minimum gap as 2 microseconds
- 4 – Configures the minimum gap as 4 microseconds
- 8 – Configures the minimum gap as 8 microseconds
- 16 – Configures the minimum gap as 16 microseconds
- auto – Auto configures the minimum gap depending on the platform and radio type (default setting)

### aggregation amsdu [rx-only|tx-rx]

**amsdu**

Configures Aggregated MAC Service Data Unit (AMSDU) frame aggregation parameters. AMSDU aggregation collects Ethernet frames addressed to a single destination. But, unlike AMPDU, it wraps all frames in a single 802.11n frame.

**rx-only**

Supports the receipt of AMSDU aggregated frames only (default setting)

**tx-rx**

Supports the transmission and receipt of AMSDU aggregated frames
Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#aggregation ampdu tx-only

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
  interface radio1
    aggregation ampdu tx-only
    aeroscout forward
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

| no                  | Disables 802.11n aggregation parameters |
7.1.34.4 airtime-fairness

Enables fair access to the medium for wireless clients based on their airtime usage (i.e. regardless of whether the client is a high-throughput (802.11n) or legacy client). This option is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

airtime-fairness {prefer-ht} {weight <1-10>}

Parameters

- airtime-fairness {prefer-ht} {weight <1-10>}

<table>
<thead>
<tr>
<th>airtime-fairness</th>
<th>Enables fair access to the medium for wireless clients based on their airtime usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefer-ht</td>
<td>Optional. Prioritizes high throughput (802.11n) clients over clients with slower throughput (802.11 a/b/g) and legacy clients</td>
</tr>
<tr>
<td>weight &lt;1-10&gt;</td>
<td>Optional. Configures the relative weightage for 11n clients over legacy clients.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-10&gt; – Sets a weightage ratio for 11n clients from 1 - 10</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#airtime-fairness prefer-ht weight 6

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  airtime-fairness prefer-ht weight 6
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

no Disable fair access for wireless clients (provides access on a round-robin mode)
7.1.34.4.5 antenna-diversity

Configure transmit antenna diversity for non-11n transmit rates.

Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
antenna-diversity

Parameters
None

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-diversity

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

no | Uses single antenna for non-11n transmit rates
7.1.34.4.6 antenna-downtilt

Enables the Advanced Element Panel Technology (ADEPT) antenna mode. The ADEPT mode increases the probability of parallel data paths enabling multiple spatial data streams. This option is disabled by default.

Supported in the following platforms:
- Access Point — AP7161, AP7181

**NOTE:** This feature is not supported on AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, and RFS4011.

**Syntax**

```
antenna-downtilt
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-downtilt

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aerocount forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the ADEPT antenna mode</td>
</tr>
</tbody>
</table>
7.1.34.4.7 antenna-elevation

`interface-config-radio-instance`

Configures an antenna's elevation gain. Antenna gain is the ratio of an antenna's radiation intensity in a given direction to the intensity produced by a no-loss, isotropic antenna radiating equally in all directions. An antenna's gain along the horizon and at an elevation of 30 degree may vary. The elevation gain is defined as the maximum antenna gain at 30 to 150 degrees above the horizon. If elevation gain is configured, the transmit (TX) power calculations maximize the allowable TX power for an elevation below 30 degree.

Access Points must conform to U.S. Federal Communications Commission's (FCC) limitations. FCC has now stipulated a 21dBm Effective Isotropic Radiated Power (EIRP) limit for power directed 30 degrees above the horizon.

For Zebra-supplied antennas, compatible with 5.0 GHz on the AP7562 access point, refer to the Antenna Guide for "Elevation Gain" information. If using a third-party antenna, it is required that you obtain the antenna-elevation gain information from the antenna manufacturer.

The elevation gain should be configured if the access point:

- Is deployed outdoors, and
- Is used with a dipole antenna (panel antenna and polarized antenna are for point to point only, and are excluded from this requirement), and
- Is transmitting in the 5.15 - 5.25 GHz Unlicensed National Information Infrastructure-1 (UNII-1) band.

Professional Installers must complete the following steps to ensure compliance with the FCC rule:

1. Configure the antenna type. For example:
   `ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#service antenna-type dipole`

2. Configure the antenna peak gain. For example:
   `ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-gain 7.0`

3. Configure the antenna placement. For example:
   `ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#placement outdoor`

4. Configure the antenna elevation gain. For example:
   `ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-elevation 5.0`

After the professional installer enters the antenna type, gain, placement, and elevation gain using the CLI as outlined above, the firmware will use this information and hardcoded maximum limits determined during testing (See Annex C in FCC Report #FR4D0448AB) to limit the EIRP below 21dBm for outdoor use in UNII-1 band. The antenna information is provided in the Installation guide and antenna guide.

Supported in the following platforms:
- Access Points — AP7562

Syntax

`antenna-elevation <-30.0-36.0>`

---

**NOTE:** The antenna elevation gain feature is supported only on the AP7562 model access point.

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>antenna-elevation &lt;-30.0-36.0&gt;</td>
</tr>
</tbody>
</table>

- Configures the antenna elevation gain from -30.0 - 36.0 dB. Refer to the antenna specifications for antenna-elevation gain information.
  - The default value is 0 dB.
## Examples

```bash
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-elevation 5.0

ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#show context interface radio2
  antenna-elevation 5.0
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets antenna elevation gain to default (0 dB)</td>
</tr>
</tbody>
</table>
### 7.1.34.8 antenna-gain

Configure the antenna gain for the selected radio.

Antenna gain is the ability of an antenna to convert power into radio waves and vice versa. The access point or wireless controller's *Power Management Antenna Configuration File* (PMACF) automatically configures the access point or wireless controller's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point or wireless controller calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. It is recommended that only a professional installer set the antenna gain.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
antenna-gain <0.0-15.0>
```

**Parameters**

- `antenna-gain <0.0-15.0>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>antenna-gain</td>
<td>Sets the antenna gain from 0.0 - 15.0 dBi. The default is 0.00 dBi.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-gain 12.0
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airt ime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

- `no` Resets the radio's antenna gain parameter
7.1.34.4.9 antenna-mode

    interface-config-radio-instance

Configures the antenna mode (the number of transmit and receive antennas) on the access point. This command sets the number of transmit and receive antennas on the access point. The 1x1 mode is used for transmissions over just the single -A- antenna, 1xALL is used for transmissions over the -A- antenna and all three antennas for receiving. The 2x2 mode is used for transmissions and receipts over two antennas for dual antenna models. 3x3x3 is used for transmissions and receipts over three antennas for AP81XX models. The default setting is dynamic based on the access point model deployed and its transmit power settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
antenna-mode [1*1|1*ALL|2*2|3*3|default]

Parameters
- antenna-mode [1*1|1*ALL|2*2|default]

<table>
<thead>
<tr>
<th>antenna-mode</th>
<th>Configures the antenna mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*1</td>
<td>Uses only antenna A to receive and transmit</td>
</tr>
<tr>
<td>1*ALL</td>
<td>Uses antenna A to transmit and receives on all antennas</td>
</tr>
<tr>
<td>2*2</td>
<td>Uses antennas A and C for both transmit and receive</td>
</tr>
<tr>
<td>3*3</td>
<td>Uses antenna A, B, and C for both transmit and receive</td>
</tr>
<tr>
<td>default</td>
<td>Uses default antenna settings. This is the default setting.</td>
</tr>
</tbody>
</table>

Usage Guidelines
To support STBC feature on AP71XX profile, the antenna-mode should not be configured to 1*1.

Examples
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-mode 2x2
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context interface radio1
  antenna-gain 12.0
  aggregation amdu tx-only
  aeroscout forward
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands
- no
  Resets the radio antenna mode (the number of transmit and receive antennas) to its default
### 7.1.34.4.10 assoc-response

*interface-config-radio-instance*

Configures the parameters determining whether the access point ignores or responds to an association/authorization request.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

`assoc-response [deny-threshold <1-12> | rssi-threshold <-128--40>]`

**Parameters**

- `assoc-response [deny-threshold <1-12> | rssi-threshold <-128--40>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assoc-response</td>
<td>Configures the following thresholds, based on which the AP ignores or responds to an association/authorization request: deny-threshold and rssi-threshold. Both these options are disabled by default.</td>
</tr>
<tr>
<td>deny-threshold &lt;1-12&gt;</td>
<td>Configures the number of times the AP ignores association/authorization requests, if the RSSI is below the configured RSSI threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-12&gt;</code> – Specify a value from 1 - 12.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The AP always ignores association/authorization requests when deny-threshold is not specified and rssi-threshold is specified.</td>
</tr>
<tr>
<td>rssi-threshold &lt;-128--40&gt;</td>
<td>Configures the RSSI threshold. If the RSSI is lower than the threshold configured here, the AP ignores the association/authorization request.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;128--40&gt;</code> – Specify the RSSI threshold from -128 - -40 dBi.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-71XXTestProfile-if-radio1)#assoc-response rssi-threshold -128
```

```
rfs7000-37FABE(config-profile-71XXTestProfile-if-radio1)#show context interface radio1
assoc-response rssi-threshold -128
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the RSSI threshold, based on which an association/authorization request is either ignored or responded.</td>
</tr>
</tbody>
</table>
7.1.34.11 association-list

Associates an existing global association list with this radio interface

An association ACL is a policy-based access control list (ACL) that either prevents or allows wireless clients from connecting to a managed access point radio. An ACL is a sequential collection of permit and deny rules that apply to incoming and outgoing packets. When a packet is received on an interface, the controller, service platform, or access point compares the fields in the packet against the applied ACLs to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified in the ACL, it is dropped.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
association-list global <GLOBAL-ASSOC-LIST-NAME>
```

**Parameters**

- `association-list global <GLOBAL-ASSOC-LIST-NAME>`

**Examples**

```
rfs4000-880DA7(config-profile-test-if-radio1)#association-list global test
rfs4000-880DA7(config-profile-test-if-radio1)#show context interface radio1
association-list global test
rfs4000-880DA7(config-profile-test-if-radio1)#
```

**Related Commands**

```
no
```

Removes the global association list associated with this radio interface
7.1.34.4.12 beacon

Configure radio beacon parameters

A beacon is a packet broadcasted by adopted radios to keep the network synchronized. Included in a beacon is information, such as the WLAN service area, the radio address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a Delivery Traffic Indication Message (DTIM). Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter sensitive.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

beacon [dtim-period|period]
beacon dtim-period [<1-50]|bss
beacon dtim-period [<1-50]|bss <1-16> <1-50>
beacon period [50|100|200]

Parameters
- beacon dtim-period [<1-50]|bss <1-16> <1-50>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtim-period</td>
<td>Configures the radio DTIM interval. A DTIM is a message that informs wireless clients about the presence of buffered multicast or broadcast data. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</td>
</tr>
<tr>
<td>&lt;1-50&gt;</td>
<td>Configures a single value to use on the radio. Specify a value between 1 and 50.</td>
</tr>
<tr>
<td>bss &lt;1-16&gt;</td>
<td>Configures a separate DTIM for a Basic Service Set (BSS) on this radio interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-16&gt; – Sets the BSS number from 1 - 16</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-50&gt; – Sets the BSS DTIM from 1 - 50. The default is 2.</td>
</tr>
<tr>
<td>period [50</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>• 50 – Configures 50 K-uSec interval between beacons</td>
</tr>
<tr>
<td></td>
<td>• 100 – Configures 100 K-uSec interval between beacons (default)</td>
</tr>
<tr>
<td></td>
<td>• 200 – Configures 200 K-uSec interval between beacons</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#beacon dtim-period bss 2 20
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#beacon period 50

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
  interface radio1
    beacon period 50
    beacon dtim-period bss 1 2
    beacon dtim-period bss 2 20
    beacon dtim-period bss 3 2
    --More--
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the configured beacon parameters</td>
</tr>
</tbody>
</table>
### 7.1.34.4.13 bridge

**interface-config-radio-instance**

Configures client-bridge related parameters if the selected radio is functioning as a client bridge.

---

**NOTE:** The client-bridge functionality is supported only on interface radio 2 of AP6522 and AP6562 model access points.

---

**Supported in the following platforms:**
- Access Points — AP6522, AP6562

**Syntax**

```
```

**Parameters**


**bridge**

Configures client-bridge related parameters.

Use this command to configure client-bridge parameters on the radio interface that has been configured to function as a bridge. To enable client-bridge functionality, on the AP's radio interface, set the rf-mode to bridge.

**Note:** When enabled as a client bridge, the radio by default maps bridged traffic to VLAN 1.

**authentication-type [eap|none]**

Configures the authentication type for the WLAN to which the radio 2 connects. The options are:
- eap – Uses EAP authentication (802.1X). If using EAP, use the ’eap’ keyword to configure EAP related parameters.
- none – Uses no authentication. This is the default setting.

**channel-dwell-time <50-2000>**

Configures the time, in microseconds, the radio dwells on each channel when the bridge scans for an AP to connect to.

- <50-2000> – Specify a value from 50 - 2000 microseconds. The default is 150 microseconds.

**channel-list [2.4GHz|5GHz] <LIST>**

Configures the list of 2.4 GHz and 5.0 GHz channels the radio scans to identify a AP to connect to.

- 2.4GHz <LIST> – Configures the 2.4 GHz channel list
- 5GHz <LIST> – Configures the 5.0 GHz channel list
- <LIST> – Provide the list of channels separated by commas.

**Note:** By default the radio scans all permitted 2.4 GHz and 5.0 GHz channels. To prevent the scanning of a particular band, execute the `bridge > channel-list 2.4 GHz` or `bridge > channel-list 5.0 GHz` command with no channel list assigned in the profile.
<table>
<thead>
<tr>
<th>connect-through-bridges</th>
<th>Enables the inclusion of APs (having a bridge radio), when scanning for APs to connect to. When enabled, allows daisy-chaining bridges. This option is disabled by default.</th>
</tr>
</thead>
</table>
| eap [password [0|2]<PASSWORD>] type [peap-mschapv2|tls]|Configures EAP authentication parameters  
- password [0|2]<PASSWORD>] – Configures the EAP password. The password type depends on the EAP authentication type configured.  
PEAP-MSCHAPv2 - PEAP password (example, zebra)  
TLS – PKCS #12 certificate secret  
Use of EAP-TLS authentication is recommended since it is stronger than PEAP-MSCHAPv2.  
For more information on EAP TLS authentication and client-side certificates, see EAP Authentication.  
Use one of the following options to configure the password:  
- 0 – Configures a clear text password. Enter the password.  
- 2 – Configures an encrypted password. Enter the password.  
- <PASSWORD> – Enter the password.  
- type [peap-mschapv2|tls] – Configures the EAP authentication type. The options are:  
PEAP-MSCHAPv2 – Configures the EAP authentication type as PEAP-MSCHAPv2. This is the default setting.  
TLS – Configures the EAP authentication type as TLS  
- username <USERNAME> – Configures the EAP username. The password type depends on the EAP authentication type configured.  
PEAP-MSCHAPv2 – PEAP username (example client-bridge)  
TLS – Username in the CN field of the installed PKCS #12 client certificate (example client-bridge@example.com)  
- <USERNAME> – Specify the EAP username |
| encryption-type [ccmp|none|tkip] | Configures the encryption type for the WLAN to which the radio 2 connects. The options are:  
- ccmp – Uses WPA/WPA2 CCMP encryption  
- none – Uses no encryption method. This is the default setting.  
- tkip – Uses WPA/WPA2 TKIP encryption  
**Note:** As per the 802.11n amendment, 802.11n data-rates can be achieved only if the encryption-type is set to CCMP or none. |
| inactivity-timeout <0-864000> | Configures the inactivity timeout in seconds. If a frame is not received from a wired/wireless client for this amount of time specified here, the client is deleted.  
- <0-864000> – Specify a value from 0 - 864000 seconds. The default is 600 seconds. |
| keepalive [frame-type [null-data|wnmp]] interval <0-36000>] | Configures the keep-alive frame type and interval  
- frame-type – Configures the keep-alive frame type sent on behalf of the bridged client. The options are:  
null-data – Transmits 802.11 NULL data frames. This is the default setting  
wnmp – Transmits Wireless Network Management Protocol (WNMP) multicast packet  
- interval <0-36000> – Configures the interval, in seconds, between two successive keep-alive frame transmission.  
- <0-36000> – Specify a value from 0 - 36000 seconds. The default is 300 seconds. |
| max-clients <1-14> | Configures the maximum number of clients bridged by the access point  
- <1-14> – Specify a value from 1 - 14. The default is 14. |
### Usage Guidelines EAP Authentication

The AP6522/AP6562 client bridges, using EAP-TLS for WLAN authentication, require client-side X.509 certificates to be deployed and installed on them. These certificates contain the PKCS #12 personal information exchange syntax standards that define a file format used to store private keys with accompanying public key certificates, which are protected using a password-based symmetric key.

The PKCS #12 certificate must be installed prior to enabling EAP-TLS on the client bridge radio. The certificate can be transferred to an AP6522/AP6562 client bridge either manually (using FTP, SFTP, or TFTP), or as part of the staging process via MiNT. If the client bridges are already associated and authenticated to the infrastructure WLAN, use PSK or PEAP-MSCHAPv2 to transfer the PKCS #12 certificate.

The following points should be taken into consideration when deploying PKCS #12 client-side certificates:

1. The exported PKCS #12 certificate must include the Private Key. When exporting the PKCS #12 certificate from Microsoft Certificate Services the option Allow private key to be exported must be selected.
2. The EAP username must be defined in the CN field in the subject of the X.509 certificate using the username@example.com or anonymous format.
3. The username in the CN field of the X.509 client-side certificate should match the username defined under radio 2 using the bridge > EAP > username command. For example if the username in the CN field is set to client-bridge@tmelabs.local, the EAP username should also be set to client-bridge@tmelabs.local.
4. The password used to secure the PKCS #12 certificate during export must be defined under radio 2 using bridge > EAP > password command. The bridge EAP password value must match the export password for the AP6522/AP6562 client bridge to access the PKCS #12 file.

### Table

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| on-link-loss shutdown-other-radio <1-1800> | Enables the access point to adopt the following behavior when the client bridge link goes down:  
  - shutdown-other-radio – Shuts down the non-bridge radio (radio 1) in order to push associated clients to search for and associate with other access points having backhaul connectivity. This option is disabled by default.  
  - <1-1800> – Configures the time, in seconds, for which the non-bridge radio is shut down after the client bridge link goes down. Specify a value from 1 - 1800 seconds. |
| on-link-up refresh-vlan-interface | Configures the access point’s behavior when the client bridge link goes up  
  - refresh-vlan-interface – Enables the radio to refresh the client bridge’s VLAN interface, and if using a DHCP assigned IP address, causes a DHCP renew. This option is enabled by default. |
| roam-criteria [missed-beacons <1-60>] [rssi-threshold <128--40>] | Configures this client bridge’s roaming parameters  
  - missed-beacons <1-60> – Configures the interval, in seconds, between two successive missed beacons (beacons not received from the bridged client)  
  - <1-60> – Specify a value from 1 - 60 seconds. The default is 20 seconds.  
  - rssi-threshold <128--40> – Configures the minimum signal strength, received from target AP, for the bridge connection to be maintained before roaming  
  - <128--40> – Specify a value from -128 - -40. The default is -75. |
| ssid <SSID> | Configures the SSID of the AP to which this client bridge connects  
  - <SSID> – Specify the SSID. The WLAN should be existing and configured. |
| wpa-wpa2 psk [0|2]<LINE> | Configures the WPA/WPA2 pre-shared key (psk)  
  - 0 – Configures clear text psk  
  - 2 – Configures encrypted psk  
  - <LINE> – Enter the key  
  **Note:** Pre-shared keys are valid only when the authentication-type is set to none and the encryption-type is set to tkip or ccmp.  
  **Note:** The PSK should be 8 - 32 characters in length. |
In a managed WLAN, multiple client-bridges can either use a common X.509 client-side certificate, or individual, unique certificates for each client bridge. If using unique certificates, upload individual PKCS #12 certificate on each AP6522/AP6562 access point. Additionally, if the individual X.509 certificates have unique CN fields or passwords, define a unique bridge EAP username and bridge EAP password parameters as device overrides.

The PEAP-MSCHAPv2 authentication, on the other hand, uses usernames and passwords for RADIUS authentication. These usernames and passwords can be either common or unique to every client-bridge. If using unique credentials, ensure that the AP6522/AP6562 client bridge’s unique username and password are defined in the back-end user directory. Also apply device overrides to each AP6522/AP6562 AP by specifying unique bridge EAP username and bridge EAP password.

Deploying unique credentials or X.509 client-side certificates is recommended, because it is easy to revoke a single user account or X.509 certificate in case an individual client bridge is stolen or compromised. In addition, unique usernames simplify identification of client-bridges within the infrastructure WLAN.

The AP6522/AP6562 access points can be deployed as standalone or centrally-managed client bridges. For steps to configuring client bridges, see Configuring Standalone Client Bridges AND Configuring Centrally Managed Client Bridges.

Examples

nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#rf-mode bridge
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge ssid techPubs
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge authentication-type eap
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge eap type tls
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge eap password 0 testuser@123
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge eap username testuser
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge encryption-type ccmp
nx4500-5CFA8E(config-profile-testAP6562-if-radio2)#bridge on-link-loss shutdown-other-radio 500

Examples Configuring Standalone Client Bridges

Following are the recommended best practices for deploying standalone client bridges. These configurations are made on the access point.

Modify the default firewall policy.

1. Access the default firewall config context.
   \[AP6522-E91438(config)#firewall-policy default\]

2. Disable DoS detection.
   \[AP6522-E91438(config-fw-policy-default)#no ip dos\]

3. Disable IP MAC conflict detection.
   \[AP6522-E91438(config-fw-policy-default)#no ip-mac routing conflict\]

4. Disable stateful packet inspection.
   \[AP6522-E91438(config-fw-policy-default)#no stateful-packet-inspection-12\]
5. Disable layer 3 firewall.
   AP6522-E91438(config-fw-policy-default)#no firewall enable

6. Exit the default firewall config context and commit and write changes to memory.
   AP6522-E91438(config-fw-policy-default)#exit
   AP6522-E91438(config-fw-policy-default)#commit write

Modify the default management policy.
1. Access the default management policy config context.
   AP6522-E91438(config)#management-policy default

2. Disable management services that are not required.
   AP6522-E91438(config-management-policy-default)#no https server
   AP6522-E91438(config-management-policy-default)#no snmp-server manager all

3. Restrict remote access to specific host(s) or subnet(s).
   AP6522-E91438(config-management-policy-default)#restrict-access subnet 192.168.10.0/24

4. Exit the default management policy config context and commit and write changes to memory.
   AP6522-E91438(config-management-policy-default)#exit
   AP6522-E91438(config)#commit write

Modify the default RF Domain policy.
1. Access the default RF Domain config context.
   AP6522-E91438(config)#rf-domain default

2. Define location, contact, country code, and timezone.
   AP6522-E91438(config-rf-domain-default)#location "Johnson City TN"
   AP6522-E91438(config-rf-domain-default)#contact "kmarshall@Zebrasolutions.com"
   AP6522-E91438(config-rf-domain-default)#country-code us
   AP6522-E91438(config-rf-domain-default)#timezone EST5EDT

3. Exit the default RF Domain config context and commit and write changes to memory.
   AP6522-E91438(config-rf-domain-default)#exit
   AP6522-E91438(config)#commit write

Modify the default AP6522 profile.
1. Access the default AP6522 profile config context.
   AP6522-E91438(config)#profile AP6522 default-AP6522

2. Modify level 1 MiNT area ID (any value other than 1).
   AP6522-E91438(config-profile-default-AP6522)#mint level 1 area-id 65535

3. Assign DNS name server, Domain name, and NTP server.
   AP6522-E91438(config-profile-default-AP6522)#ip name-server 192.168.10.6
   AP6522-E91438(config-profile-default-AP6522)#tmelabs.local
   AP6522-E91438(config-profile-default-AP6522)#ntp server 192.168.10.1

   AP6522-E91438(config-profile-default-AP6522)#interface radio 1
   AP6522-E91438(config-profile-default-AP6522-if-radio1)#shutdown
   AP6522-E91438(config-profile-default-AP6522-if-radio1)#exit

5. Configure radio 2 as client bridge radio (example for pre-shared key).
   AP6522-E91438(config-profile-default-AP6522)#interface radio 2
   AP6522-E91438(config-profile-default-AP6522-if-radio2)#rf-mode bridge
   AP6522-E91438(config-profile-default-AP6522-if-radio2)#bridge ssid TMELABS-PSK
   AP6522-E91438(config-profile-default-AP6522-if-radio2)#bridge authentication-type none
6. Configure radio 2 as client bridge radio (example for PEAP-MSCHAPv2).

   652-E91438 (config-profile-default-AP6522)#interface radio 2
   652-E91438 (config-profile-default-AP6522-if-radio2)#rf-mode bridge
   652-E91438 (config-profile-default-AP6522-if-radio2)#bridge ssid TMELABS-DOT1X
   652-E91438 (config-profile-default-AP6522-if-radio2)#bridge authentication-type eap
   652-E91438 (config-profile-default-AP6522-if-radio2)#bridge encryption-type ccmp
   652-E91438 (config-profile-default-AP6522-if-radio2)#bridge eap type tls
   652-E91438 (config-profile-default-AP6522-if-radio2)#bridge eap username cb@tmelabs.local
   652-E91438 (config-profile-default-AP6522-if-radio2)#bridge eap password zebra

7. Exit the default AP6522 profile config context and commit and write changes to memory.

   652-E91438 (config-profile-default-AP6522)#exit
   652-E91438(config)# commit write

**Apply AP6522 device overrides.**

1. Access AP6522's device config context.

   652-E91438 (config)#AP6522 B4-C7-99-E9-14-38

2. Configure access point's hostname.

   652-E91438 (config-device-B4-C7-99-E9-14-38)#hostname AP6522-CB1

3. Exit the AP6522's device config context and commit and write changes to memory.

**Configure static IPv4 address and default gateway on the AP6522 client bridge.**

1. Access AP6522’s device config context.

   652-CB1(config)#AP6522 B4-C7-99-E9-14-38

2. Define a *Switched Virtual Interface* (SVI) for VLAN 1 for Management.

   652-CB1(config-device-B4-C7-99-E9-14-38)#interface vlan 1

3. Define a IPv4 address and mask.

   652-CB1(config-device-B4-C7-99-E9-14-38-if-vlan1)#ip address 192.168.13.100/24

4. Define a default gateway.

   652-CB1(config-device-B4-C7-99-E9-14-38-if-vlan1)#ip default-gateway 192.168.13.1

5. Exit the AP6522’s device config context and commit and write changes to memory.

   652-CB1(config-device-B4-C7-99-E9-14-38)#exit
   652-CB1(config)#commit write

**Define encryption password and enable inline password encryption.**

1. Define encryption password.

   652-CB1(config)#password-encryption secret 2 zebra

2. Enable inline password encryption.

   652-CB1(config)#inline-password-encryption

3. Commit and write changes to memory.

   652-CB1(config)#commit write

**Pre-stage AP6522 client bridge prior to deployment.**
1. Pre-stage the AP6522 client bridge by applying all parameters required to connect to the infrastructure WLAN and manage the device.

   AP6522-CB1(config-device-B4-C7-99-E9-14-38)#use profile default-AP6522
   AP6522-CB1(config-device-B4-C7-99-E9-14-38)#use rf-domain default

**Configuring Centrally Managed Client Bridges**

Following are the recommended best practices for deploying centrally-managed client bridges. These configurations are made on the staging controller and applied to the client bridge AP on adoption.

**Modify the default firewall policy.**

1. Access the default firewall config context.

   CBMGR-ACTIVE(config)#firewall-policy default

2. Disable DoS detection.

   CBMGR-ACTIVE(config-fw-policy-default)#no ip dos

3. Disable IP MAC conflict detection.

   CBMGR-ACTIVE(config-fw-policy-default)#no ip-mac routing conflict

4. Disable layer 2 stateful packet inspection.

   CBMGR-ACTIVE(config-fw-policy-default)#no stateful-packet-inspection-l2

5. Disable layer 3 firewall.

   CBMGR-ACTIVE(config-fw-policy-default)#no firewall enable

6. Exit the default firewall config context and commit and write changes to memory.

**Create a user-defined management policy.**

1. Create a new management policy and enter its config context.

   CBMGR-ACTIVE(config)#management-policy CLIENT-BRIDGES

2. Define an admin user and assign a password to this user.

   CBMGR-ACTIVE(config-management-policy-CLIENT-BRIDGES)#user admin password zebra role superuser access all

3. Disable management services that are not required.

   CBMGR-ACTIVE(config-management-policy-CLIENT-BRIDGES)#no http server
   CBMGR-ACTIVE(config-management-policy-CLIENT-BRIDGES)#no snmp-server manager all

4. Enable SSH.

   CBMGR-ACTIVE(config-management-policy-CLIENT-BRIDGES)#ssh

5. Restrict remote access to specific host(s) or subnet(s).

   CBMGR-ACTIVE(config-management-policy-CLIENT-BRIDGES)#restrict-access subnet 192.168.10.0/24

6. Exit the CLIENT-BRIDGES management policy config context and commit and write changes to memory.

   CBMGR-ACTIVE(config-management-policy-CLIENT-BRIDGES)#exit
   CBMGR-ACTIVE(config)#commit write

**Create a user-defined RF Domain.**

1. Create a new RF Domain and enter its config context.

   CBMGR-ACTIVE(config)#rf-domain STORE201

2. Define location, contact, country code, and timezone.

   CBMGR-ACTIVE(config-rf-domain-STORE201)#location "Johnson City TN"
   CBMGR-ACTIVE(config-rf-domain-STORE201)#contact "kmarshall@Zebрасolutions.com"
   CBMGR-ACTIVE(config-rf-domain-STORE201)#country-code us
   CBMGR-ACTIVE(config-rf-domain-STORE201)#timezone EST5EDT
3. Exit the STORE201 RF Domain config context and commit and write changes to memory.
   
   CBMGR-ACTIVE(config-rf-domain-STORE201)#exit
   CBMGR-ACTIVE(config)#commit write

Create a user-defined client-bridge AP6522 profile.
1. Create a new AP6522 profile and enter its config context.
   
   CBMGR-ACTIVE(config)#profile AP6522 cb-AP6522

2. Modify level 1 MiNT area ID (any value other than 1).
   
   CBMGR-ACTIVE(config-profile-CB-AP6522)#mint level 1 area-id 65535

3. Assign DNS name server, Domain name, and NTP server.
   
   CBMGR-ACTIVE(config-profile-CB-AP6522)#ip name-server 192.168.10.6
   CBMGR-ACTIVE(config-profile-CB-AP6522)#tmelabs.local
   CBMGR-ACTIVE(config-profile-CB-AP6522)#ntp server 192.168.10.1

4. Map the user-defined management policy 'CLIENT-BRIDGES' to this AP6522 profile.
   
   CBMGR-ACTIVE(config-profile-CB-AP6522)#use management-policy CLIENT-BRIDGES

5. Define a SVI for VLAN 1 with DHCP enabled for Management & Adoption.
   
   CBMGR-ACTIVE(config-profile-CB-AP6522)#interface vlan 1
   CBMGR-ACTIVE(config-profile-CB-AP6522-if-vlan1)#ip address dhcp
   CBMGR-ACTIVE(config-profile-CB-AP6522-if-vlan1)#ip dhcp client request options all
   CBMGR-ACTIVE(config-profile-CB-AP6522-if-vlan1)#exit

   
   CBMGR-ACTIVE(config-profile-CB-AP6522)#interface radio 1
   CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio1)#shutdown
   CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio1)#exit

7. Configure radio 2 as client bridge radio.
   
   a. Radio 2 as client bridge radio: example for pre-shared key
      
      CBMGR-ACTIVE(config-profile-CB-AP6522)#interface radio 2
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#rf-mode bridge
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge ssid TMELABS-PSK
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge authentication-type none
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge encryption-type ccmp
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge wpa-wpa2 psk zebra12345
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#exit

   b. Radio 2 as client bridge radio: example for PEAP-MSCAPv2
      
      CBMGR-ACTIVE(config-profile-CB-AP6522)#interface radio 2
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#rf-mode bridge
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge ssid TMELABS-DOT1X
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge authentication-type eap
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge encryption-type ccmp
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge eap type tls
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge eap username cb@tmelabs.local
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge eap password zebra
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#exit

   c. Radio 2 as client bridge radio: example for EAP-TLS
      
      CBMGR-ACTIVE(config-profile-CB-AP6522)#interface radio 2
      CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#rf-mode bridge
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge ssid TMELABS-DOT1X
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge authentication-type eap
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge encryption-type ccmp
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge eap type tls
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge eap username cb@tmelabs.local
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#bridge eap password zebra
CBMGR-ACTIVE(config-profile-CB-AP6522-if-radio2)#exit

8. Exit the AP6522 profile 'CB-AP6522' config context and commit and write changes to memory.
   CBMGR-ACTIVE(config-profile-CB-AP6522)#exit
   CBMGR-ACTIVE(config)#commit write

Define encryption password and enable inline password encryption.
1. Define encryption password.
   CBMGR-ACTIVE(config)#password-encryption secret 2 zebra
2. Enable inline password encryption.
   CBMGR-ACTIVE(config)#inline-password-encryption
3. Commit and write changes to memory.
   CBMGR-ACTIVE(config)#commit write

Configuring centralized controller discovery.
For centrally-managed deployments, AP6522/AP6562 client bridges can discover centralized controllers (active and standby) and establish level 2 MiNT links using static controller host entries or DHCP options.

a. DHCP options
   AP6522/AP6562 client bridges support dynamic layer 3 discovery using DHCP. DHCP can be used to assign network addressing in addition to sending Zebra vendor-specific DHCP option 191, which enables AP6522/AP6562 client bridges to automatically discover and adopt to the centralized controllers. DHCP option 191 is supplied as ASCII/string to the AP6522/AP6562 client bridges in a DHCP offer, and each string includes the IPv4 addresses of the active and standby centralized controllers, Pool, and MiNT routing level. To support the AP6522/AP6562 client bridges, DHCP Option 191 must be assigned to each DHCP Pool providing addresses to the AP6522/AP6562 client bridges.

b. Layer 3 controller-host discovery using controller-host configuration
   AP6522/AP6562 client bridges support static layer 3 discovery using controller hosts defined in the user-defined AP6522 or AP6562 profiles. Controller hosts are typically used for deployments when AP6522/AP6562 client bridges are assigned static network addressing or when DHCP options cannot be deployed. The AP6522 or AP6562 profile includes up to two controller host entries. The first entry defines the active controller’s IPv4 address (pool 1), while the second entry defines the standby controller’s IPv4 address (pool 2). The MiNT routing level is set 2 for both hosts.

Access the user-defined client-bridge AP6522 profile.
CBMGR-ACTIVE(config)#profile AP6522 CB-AP6522

Define active and standby centralized controller host entries.
CBMGR-ACTIVE(config-profile-CB-AP6522)#controller host 192.168.20.90 pool 1 level 2
CBMGR-ACTIVE(config-profile-CB-AP6522)#controller host 192.168.20.91 pool 2 level 2

Exit then commit and write the changes.
CBMGR-ACTIVE(config-profile-CB-AP6522)#exit
CBMGR-ACTIVE(config)#commit write
Auto-provisioning client-bridge access points.

In a centrally-managed deployment, each AP6522/AP6562 client bridge is assigned a user-defined profile and RF Domain upon initial adoption to the centralized controller. It is an auto-provisioning policy, mapped to the centralized controller’s profile, which assigns the user-defined profile and RF Domain to the new AP6522/AP6562 client bridges. The auto-provisioning policy includes IP=match criteria and corresponding adopt rules. These rules determine the profile and RF Domain to assign to each new AP6522/AP6562 client bridge matching the criteria provided.

1. Create a user-defined auto provisioning policy and enter its config context.

   CBMGR-ACTIVE(config)#auto-provisioning-policy DATACENTER

2. Define an adoption rule providing the IP match criteria and the profile and RF Domain to assign in case of a match.

   CBMGR-ACTIVE(config-auto-provisioning-policy-DATACENTER)#adopt AP6522 precedence 1 profile CB-AP6522 rf-domain STORE201 ip 192.168.21.0/24

   CBMGR-ACTIVE(config-auto-provisioning-policy-DATACENTER)#exit

3. Map the user-defined auto provisioning policy to the centralized controller profile.

   CBMGR-ACTIVE(config)#profile nx9000 DATACENTER-NX9000

   CBMGR-ACTIVE(config-profile-DATACENTER-NX9000)#use auto-provisioning-policy DATACENTER

4. Exit then centralized controller profile ‘DATACENTER-NX9000’ config context and commit and write the changes to memory.

   CBMGR-ACTIVE(config-profile-NX9000-DATACENTER)#exit

   CBMGR-ACTIVE(config)#commit write

Related Commands

| no | Removes or resets this client-bridge settings |
7.1.34.4.14 channel

interface-config-radio-instance

Configures a radio’s channel of operation

Only a trained installation professional should define the radio channel. Select Smart for the radio to scan non-overlapping channels listening for beacons from other access points. After the channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it selects the channel with the lowest average power level.

NOTE: Channels with a “w” appended to them are unique to the 40 MHz band. Channels with a “ww” appended to them are 802.11ac specific, and appear only when using an AP82XX, and are unique to the 80 MHz band.

Supported in the following platforms:
• Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4011

Syntax

channel [smart|acs|random|1|2|3|4|-------]

Parameters

• channel [smart|acs|random|1|2|3|4|-------]

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#channel 1
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radiol
  channel 1
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  .................................................................
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-mode 2x2
  antenna-diversity
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

no Resets a radio’s channel of operation
7.1.34.4.15 data-rates

Configures the 802.11 data rates on this radio

This command sets the rate options depending on the 802.11 protocol and the radio band selected. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together.

If dedicating the radio to either 2.4 or 5.0 GHz support, use the custom keyword to set a 802.11n modulation and coding scheme (MCS) in respect to the radio’s channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

Data rates are fixed and not user configurable for radios functioning as sensors.

---

**NOTE:** Use the rf-mode command to configure a radio’s mode of operation.

---

**NOTE:** The MCS-1s and MCS-2s options are available for each supported access point. However, the MCS-3s option is only available to the AP8232 model access point, and its ability to provide 3x3x3 MIMO support.

---

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom|mcs]
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]
data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54|mcs-1s|mcs-2s|mcs-3s|basic-1|basic-2|basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|basic-24|basic-36|basic-48|basic-54|basic-mcs-1s]
data-rates mcs qam-only

**Parameters**

- **data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]**

<table>
<thead>
<tr>
<th>data-rates</th>
<th>Configures the 802.11 data rates on this radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>b-only</td>
<td>Supports operation in the 802.11b mode only (applicable for 2.4 and 4.9 GHz bands)</td>
</tr>
<tr>
<td>g-only</td>
<td>Uses rates that support operation in the 802.11g mode only (applicable for 2.4 and 4.9 GHz bands)</td>
</tr>
<tr>
<td>a-only</td>
<td>Uses rates that support operation in the 802.11a mode only (applicable for 5.0 GHz band only)</td>
</tr>
<tr>
<td>bg</td>
<td>Uses rates that support 802.11b and 802.11g wireless clients (applicable for 2.4 and 4.9 GHz bands)</td>
</tr>
<tr>
<td>bgn</td>
<td>Uses rates that support 802.11b, 802.11g, and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>gn</td>
<td>Uses rates that support 802.11g and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)</td>
</tr>
<tr>
<td>an</td>
<td>Uses rates that support 802.11a and 802.11n wireless clients (applicable for 5.0 GHz band only)</td>
</tr>
<tr>
<td>default</td>
<td>Enables the default data rates according to the radio’s band of operation</td>
</tr>
<tr>
<td>custom</td>
<td>Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it’s used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11')</td>
</tr>
</tbody>
</table>

- 1 – 1-Mbps
- 2 – 2-Mbps
- 5.5 – 5.5-Mbps
- 6 – 6-Mbps
- 9 – 9-Mbps
- 11 – 11-Mbps
- 12 – 12-Mbps
- 18 – 18-Mbps
- 24 – 24-Mbps
- 36 – 36-Mbps
- 48 – 48-Mbps
- 54 – 54-Mbps
- mcs-1s – Applicable to 1-spatial stream data rates
- mcs-2s – Applicable to 2-spatial stream data rates
- mcs-3s – Applicable to 3-spatial stream data rates (supported only on AP8232 for the MIMO feature)
- basic-1 – Basic 1-Mbps
- basic-2 – Basic 2-Mbps
- basic-5.5 – Basic 5.5-Mbps
- basic-6 – Basic 6-Mbps
- basic-9 – Basic 9-Mbps
- basic-11 – Basic 11-Mbps
- basic-12 – Basic 12-Mbps
- basic-18 – Basic 18-Mbps
- basic-24 – Basic 24-Mbps
- basic-36 – Basic 36-Mbps
- basic-48 – Basic 48-Mbps
- basic-54 – Basic 54-Mbps
- basic-mcs-1s – Modulation and Coding Scheme data rates for 1 Spatial Stream

Refer to the Usage Guidelines (Supported data rates) section for 802.11an and 802.11ac MCS detailed dates rates for both with and without short guard intervals (SGI).
**Usage Guidelines (Supported data rates)**

The following table defines the 802.11n MCS for MCS 1 streams, both with and without SGI:

<table>
<thead>
<tr>
<th>MCS-1Stream Index</th>
<th>Number of Streams</th>
<th>20 MHz No SGI</th>
<th>20 MHz With SGI</th>
<th>40 MHz No SGI</th>
<th>20 MHz With SGI</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>6.5</td>
<td>7.2</td>
<td>13.5</td>
<td>15</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>13</td>
<td>14.4</td>
<td>27</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>19.5</td>
<td>21.7</td>
<td>40.5</td>
<td>45</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>26</td>
<td>28.9</td>
<td>54</td>
<td>60</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>39</td>
<td>43.4</td>
<td>81</td>
<td>90</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>52</td>
<td>57.8</td>
<td>108</td>
<td>120</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>58.5</td>
<td>65</td>
<td>121.5</td>
<td>135</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>65</td>
<td>72.2</td>
<td>135</td>
<td>150</td>
</tr>
</tbody>
</table>

The following table defines the 802.11n MCS for MCS 2 streams, both with and without SGI:

<table>
<thead>
<tr>
<th>MCS-2Stream Index</th>
<th>Number of Streams</th>
<th>20 MHz No SGI</th>
<th>20 MHz With SGI</th>
<th>40 MHz No SGI</th>
<th>20 MHz With SGI</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>13</td>
<td>14.4</td>
<td>27</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>26</td>
<td>28.9</td>
<td>54</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>39</td>
<td>43.4</td>
<td>81</td>
<td>90</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>52</td>
<td>57.8</td>
<td>108</td>
<td>120</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>78</td>
<td>86.7</td>
<td>162</td>
<td>180</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>104</td>
<td>115.6</td>
<td>216</td>
<td>240</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>117</td>
<td>130</td>
<td>243</td>
<td>270</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>130</td>
<td>144.4</td>
<td>270</td>
<td>300</td>
</tr>
</tbody>
</table>

The following table defines the 802.11n MCS for MCS 3 streams, both with and without SGI:

<table>
<thead>
<tr>
<th>MCS-3Stream Index</th>
<th>Number of Streams</th>
<th>20 MHz No SGI</th>
<th>20 MHz With SGI</th>
<th>40 MHz No SGI</th>
<th>20 MHz With SGI</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>19.5</td>
<td>21.7</td>
<td>40.5</td>
<td>45</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>39</td>
<td>43.3</td>
<td>81</td>
<td>90</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>58.5</td>
<td>65</td>
<td>121.5</td>
<td>135</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>78</td>
<td>86.7</td>
<td>162</td>
<td>180</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>117</td>
<td>130.7</td>
<td>243</td>
<td>270</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>156</td>
<td>173.3</td>
<td>324</td>
<td>360</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>175.5</td>
<td>195</td>
<td>364.5</td>
<td>405</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>195</td>
<td>216.7</td>
<td>405</td>
<td>450</td>
</tr>
</tbody>
</table>
The following table defines the 802.11ac MCS rates (theoretical throughput for single spatial streams) both with and without SGI:

<table>
<thead>
<tr>
<th>MCS Index</th>
<th>20 MHz No SGI</th>
<th>20 MHz With SGI</th>
<th>40 MHz No SGI</th>
<th>40 MHz With SGI</th>
<th>80 MHz No SGI</th>
<th>80 MHz No SGI</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>6.5</td>
<td>7.2</td>
<td>13.5</td>
<td>15</td>
<td>29.3</td>
<td>32.5</td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>14.4</td>
<td>27</td>
<td>30</td>
<td>58.5</td>
<td>65</td>
</tr>
<tr>
<td>2</td>
<td>19.5</td>
<td>21.7</td>
<td>40.5</td>
<td>45</td>
<td>87.8</td>
<td>97.5</td>
</tr>
<tr>
<td>3</td>
<td>26</td>
<td>28.9</td>
<td>54</td>
<td>60</td>
<td>117</td>
<td>130</td>
</tr>
<tr>
<td>4</td>
<td>39</td>
<td>43.3</td>
<td>81</td>
<td>90</td>
<td>175.5</td>
<td>195</td>
</tr>
<tr>
<td>5</td>
<td>52</td>
<td>57.8</td>
<td>108</td>
<td>120</td>
<td>234</td>
<td>260</td>
</tr>
<tr>
<td>6</td>
<td>58.5</td>
<td>65</td>
<td>121.5</td>
<td>135</td>
<td>263.3</td>
<td>292.5</td>
</tr>
<tr>
<td>7</td>
<td>65</td>
<td>72.2</td>
<td>135</td>
<td>150</td>
<td>292.5</td>
<td>325</td>
</tr>
<tr>
<td>8</td>
<td>78</td>
<td>86.7</td>
<td>162</td>
<td>180</td>
<td>351</td>
<td>390</td>
</tr>
<tr>
<td>9</td>
<td>N/A</td>
<td>N/A</td>
<td>180</td>
<td>200</td>
<td>390</td>
<td>433.3</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#data-rates b-only

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context interface radio1
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  ........................................................
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  --More--

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the 802.11 data rates on a radio</td>
</tr>
<tr>
<td>rf-mode</td>
<td>Configures the radio’s RF mode of operation</td>
</tr>
</tbody>
</table>
7.1.34.4.16 description

Configures the selected radio’s description that helps differentiate it from other radios with similar configurations.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

description <WORD>

**Parameters**

- description <WORD>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#description "Primary radio to use"

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context interface radio1
description Primary\ radio\ to\ use
channel 1
data-rates b-only
beacon period 50
beacon dtim-period bss 1 5
beacon dtim-period bss 2 2
beacon dtim-period bss 3 5
beacon dtim-period bss 4 5
beacon dtim-period bss 5 5
beacon dtim-period bss 6 5
beacon dtim-period bss 7 5
beacon dtim-period bss 8 5
beacon dtim-period bss 9 5
beacon dtim-period bss 10 5
beacon dtim-period bss 11 5
beacon dtim-period bss 12 5
beacon dtim-period bss 13 5
beacon dtim-period bss 14 5
beacon dtim-period bss 15 5
beacon dtim-period bss 16 5
antenna-gain 12.0
aggregation ampdu tx-only
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

- **no** Removes a radio’s description
7.1.34.4.17 dfs-rehome

Reverts to configured home channel once the Dynamic Frequency Selection (DFS) evacuation period expires.

**NOTE:** This option is applicable only if the radio’s RF mode is set to ‘5GHz-wlan’.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**
dfs-rehome {holdtime <30-3600>}

**Parameters**
- dfs-rehome {holdtime <30-3600>}

`dfs-rehome {holdtime <30-3600>}` Enables the radio to revert to the configured home channel once the DFS evacuation period expires.

- holdtime – Optional. Specifies the duration, in minutes, to stay in the new channel.
- `<30-3600>` – Specify the holdtime from 30 - 3600 minutes. The default is 90 minutes.

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#dfs-rehome holdtime 500
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#show context
  interface radiol
dfs-rehome holdtime 500
rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#
```

**Related Commands**

<table>
<thead>
<tr>
<th><strong>no</strong></th>
<th>Stays on DFS elected channel after evacuation period expires</th>
</tr>
</thead>
</table>
### 7.1.34.4.18 dynamic-chain-selection

*interface-config-radio-instance*

Enables automatic antenna mode selection. When enabled, the radio can dynamically change the number of transmit chains used (uses a single chain/antenna for frames at non-11n transmit rates). This option is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

dynamic-chain-selection

**Parameters**

None

**Examples**

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#dynamic-chain-selection
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Uses the configured transmit antenna mode for all clients</td>
</tr>
</tbody>
</table>
7.1.34.4.19 ekahau

`interface-config-radio-instance`

Enables Ekahau multicast packet forwarding. When enabled, Ekahau small, battery powered Wi-Fi tags are attached to tracked assets or assets carried by people. Ekahau processes locations, rules, messages, and environmental data and turns the information into locationing maps, alerts and reports.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

`ekahau [forward ip <IP> port <0-65535>|mac <MAC>]`

**Parameters**

- `ekahau [forward ip <IP> port <0-65535>|mac <MAC>]`

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ekahau</code></td>
<td>Enables Ekahau multicast packet forwarding on this radio</td>
</tr>
<tr>
<td><code>forward ip &lt;IP&gt; port &lt;0-65535&gt;</code></td>
<td>Enables multicast packet forwarding to the Ekahau engine</td>
</tr>
<tr>
<td><code>mac &lt;MAC&gt;</code></td>
<td>Configures the multicast MAC address to forward the Ekahau multicast packets</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#ekahau forward ip 172.16.10.1 port 3
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  ..................
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

- `no` | Uses default Ekahau multicast MAC address
7.1.34.4.20 extended-range

*interface-config-radio-instance*

Enables the extended range capability for AP7161 and AP7181 model access points. When enabled, these access points can exchange signals with their clients at greater distances without being timed out. This option is disabled by default.

Supported in the following platforms:
- Access Point — AP7161, AP7181

**Syntax**

`extended-range <1-25>`

**Parameters**

- `extended-range <1-25>`

| extended-range <1-25> | Configures extended range on this radio interface from 1 - 25 kilometers. The default is 2 km on 2.4 GHz band and 7 km on 5.0 GHz band. |

**Examples**

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#extended-range 15

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  extended-range 15
```

**Related Commands**

| `no` | Resets the extended range to default (7 km for 2.4 GHz and 5 km for 5.0 GHz) |
### 7.1.34.4.21 fallback-channel

*interface-config-radio-instance*

Configures the channel to which the radio switches in case of radar detection on the current channel.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
fallback-channel [100|100w|100ww|104|104w|104ww|108|108w|.........]
```

**Parameters**

- `fallback-channel [100|100w|100ww|104|104w|104ww|108|108w|.........]`

| fallback-channel [100|100w|........] | Configures the fallback channel. This is the channel the radio switches to in case a radar is detected on the radio's current operating channel. |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------|
| • [100|100w|100ww|... – Select the fall back channel from the available options. |

**Note:** Channels with a “w” appended to them are unique to the 40 MHz band. Channels with a “ww” appended to them are 802.11ac specific, and appear only when using an AP8232, and are unique to the 80 MHz band.

**Examples**

```
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#fallback-channel 104
```

**NOTE:** Functionality is supported only in the US regulatory domain and only a non-dfs channel can be configured as a fallback channel.

```
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#show context
interface radio2
  fallback-channel 104
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#
```

**Related Commands**

| no | Removes the fallback-channel configuration |
### 7.1.34.4.22 guard-interval

**interface-config-radio-instance**

Configures the 802.11n guard interval. A guard interval ensures distinct transmissions do not interfere with one another. It provides immunity to propagation delays, echoes and reflection of radio signals.

The guard interval is the space between transmitted characters. The guard interval eliminates *inter symbol interference* (ISI). ISI which occurs when echoes or reflections from one symbol interferes with another. Adding time between transmissions allows echoes and reflections to settle before the next symbol is transmitted. A shorter guard interval results in shorter symbol times, which reduces overhead and increases data rates by up to 10%.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

guard-interval [any|long]

**Parameters**
- guard-interval [any|long]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>guard-interval</td>
<td>Configures the 802.11n guard interval</td>
</tr>
<tr>
<td>any</td>
<td>Enables the radio to use any short (400nSec) or long (800nSec) guard interval</td>
</tr>
<tr>
<td>long</td>
<td>Enables the use of long guard interval (800nSec). This is the default setting.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#guard-interval long

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the 802.11n guard interval to default (long: 800nSec)</td>
</tr>
</tbody>
</table>
7.1.34.4.23 ldpc

- `interface-config-radio-instance`

Enables support for *Low Density Parity Check* (LDPC) codes on the radio interface.

LDPC consists of forward error correcting codes that enable error control in data transmission. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

```
ldpc
```

Parameters

None

Examples

```
rfs4000-229D58(config-profile-Test81XX-if-radio1)#ldpc
```

```
rfs4000-229D58(config-profile-Test81XX-if-radio1)#show context
   interface radio1
   ldpc
rfs4000-229D58(config-profile-Test81XX-if-radio1)#
```

Related Commands

```
no
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables LDPC support</td>
</tr>
</tbody>
</table>
7.1.34.4.24 lock-rf-mode

Retains user configured RF mode settings for the selected radio. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

lock-rf-mode

Parameters

None

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#lock-rf-mode

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  description Primary\ radio\ to\ use
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  --More--
  rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

| no | Allows Smart RF to change a radio’s RF mode settings |
### 7.1.34.4.25 max-clients

Configure the maximum number of wireless clients allowed to associate with this radio

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
max-clients <0-256>
```

**Parameters**

- `max-clients <0-256>`

**Examples**

```bash
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#max-clients 100

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
description Primary\ radio\ to\ use
channel 1
data-rates b-only
beacon period 50
beacon dtim-period bss 1 5
beacon dtim-period bss 2 2
..............................................
beacon dtim-period bss 12 5
beacon dtim-period bss 13 5
beacon dtim-period bss 14 5
beacon dtim-period bss 15 5
beacon dtim-period bss 16 5
antenna-gain 12.0
guard-interval long
aggregation ampdu tx-only
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
antenna-mode 2x2
antenna-diversity
max-clients 100
airtime-fairness prefer-ht weight 6
lock-rf-mode
extended-range 15
antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets the maximum number of wireless clients allowed to associate with a radio</td>
</tr>
</tbody>
</table>
### 7.1.34.4.26 mesh

**interface-config-radio-instance**

Use this command to configure radio mesh parameters. A *Wireless Mesh Network* (WMN) is a network of radio nodes organized in a mesh topology. It consists of mesh clients, mesh routers, and gateways.

Each radio setting can have a unique mesh mode and link configuration. This provides a customizable set of connections to other mesh supported radios within the same radio coverage area.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
mesh [client|links|portal|preferred-peer|psk]
mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2 <LINE>]| <LINE>]]
```

**Parameters**

- **mesh [client|links|portal|preferred-peer|psk]**
  - `mesh`: Configures radio mesh parameters, such as maximum number of mesh links, preferred peer device, client operations etc.
  - `client`: Enables operation as a client
    - Setting the mesh mode to 'client' enables the radio to operate as a mesh client that scans for and connects to mesh portals or nodes that are connected to portals.
  - `links <1-6>`: Configures the maximum number of mesh links a radio attempts to create
    - `<1-6>` – Sets the maximum number of mesh links from 1 - 6. The default is 6.
  - `portal`: Enables operation as a portal
    - Setting the mesh mode to 'portal' turns the radio into a mesh portal. The radio starts beaconing immediately and accepts connections from other mesh nodes, typically the node with a connection to the wired network.
  - `preferred-peer <1-6> <MAC>`: Configures a preferred peer device
    - `<1-6>` – Configures the priority at which the peer node will be added
      - When connecting to the mesh infrastructure, nodes with lower priority are given precedence over nodes with higher priority.
    - `<MAC>` – Sets the MAC address of the preferred peer device (Ethernet MAC of either a AP, wireless controller, or service platform with onboard radios)
  - `psk [0 <LINE>|2 <LINE>| <LINE>]`: Configures the pre-shared key. Ensure this key is configured on the access point when staged for mesh, and added to the mesh client and to the portal access point’s configuration on the controller or service platform.
    - `0 <LINE>` – Enter a clear text key
    - `2 <LINE>` – Enter an encrypted key
    - `<LINE>` – Enter the pre-shared key
      - Pre-shared keys should be 8 - 64 characters in length.
Examples
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#mesh client

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
  interface radio1
      description Primary\ radio\ to\ use
      channel 1
      data-rates b-only
      mesh client
      beacon period 50
      --More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

| no      | Disables mesh mode operation of the selected radio |
7.1.34.4.27 meshpoint

Maps an existing meshpoint to this radio

Use this command to assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

meshpoint <MESHPOINT-NAME> {bss <1-16>}

Parameters

- meshpoint <MESHPOINT-NAME> {bss <1-16>}

<table>
<thead>
<tr>
<th>meshpoint &lt;MESHPOINT-NAME&gt;</th>
<th>Maps a meshpoint to this radio. Specify the meshpoint name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>bss &lt;1-16&gt;</td>
<td>Optional. Specifies the radio’s BSS where this meshpoint is mapped</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#meshpoint test bss 7
rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#show context interface radio1
  meshpoint test bss 7
rfs7000-37FABE(config-profile-ap71xxTest-radio1)#

Related Commands

<table>
<thead>
<tr>
<th>no</th>
<th>Disables meshpoint on the selected radio</th>
</tr>
</thead>
</table>
7.1.34.4.28 no

*interface-config-radio-instance*

Negates a command or resets settings to their default. When used in the profile/device > radio interface configuration mode, the no command disables or resets radio interface settings.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
no <PARAMETERS>
```

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Removes or reverts this radio interface’s settings based on the parameters passed |

**Usage Guidelines**

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

**Examples**

```
rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#no ?
adaptivity      Adaptivity
aeroscout       Use Default Aeroscout Multicast MAC Address
aggregation     Configure 802.11n aggregation related parameters
airtime-fairness Disable fair access to medium for clients, provide access in a round-robin mode
antenna-diversity Use single antenna for non-11n transmit rates
antenna-downtilt Reset ADEPT antenna mode
antenna-elevation Reset the antenna elevation of this radio to default
antenna-gain     Reset the antenna gain of this radio to default
antenna-mode     Reset the antenna mode (number of transmit and receive antennas) on the radio to its default
assoc-response   Configure transmission parameters for Association Response frames
association-list Configure the association list for the radio
beacon          Configure beacon parameters
bridge          Bridge rf-mode related configuration
channel         Reset the channel of operation of this radio to default
data-rates       Reset radio data rate configuration to default
description     Reset the description of the radio to its default
dfs-rehome      Stay on dfs elected channel after evacuation period expires
dynamic-chain-selection Use the configured transmit antenna mode for all clients
ekahau          Use Default Ekahau Multicast MAC Address
extended-range  Reset extended range to default
fallback-channel Clear the DFS fallback channel for this radio
guard-interval  Configure default value of 802.11n guard interval (long: 800nSec)
ldpc            Configure support for Low Density Parity Check Code
lock-rf-mode    Allow smart-rf to change rf-mode setting for this radio
max-clients     Maximum number of wireless clients allowed to associate
mesh            Disable mesh mode operation of the radio
meshpoint       Disable a meshpoint from this radio
non-unicast     Configure handling of non-unicast frames
```
off-channel-scan             Disable off-channel scanning on the radio
placement                   Reset the placement of the radio to its default
power                       Reset the transmit power of this radio to
default                     default
preamble-short               Disable the use of short-preamble on this radio
probe-response              Configure transmission parameters for Probe
radio-resource-measurement  Configure support for 802.11k Radio Resource
radio-share-mode            Configure the radio-share mode of operation for
this radio                  default
radio-mode                   Reset the RF mode of operation for this radio to
default (2.4GHz on radio1, 5GHz on radio2,
sensor on radio3)
rifs                        Configure Reduced Interframe Spacing (RIFS)
rts-threshold               Reset the RTS threshold to its default (65536)
shutdown                    Re-enable the selected interface
smart-rf                     Reset smart-rf related configuration to default
sniffer-redirect            Disable capture and redirection of packets
stbc                        Configure Space-Time Block Coding (STBC)
parameters                  parameters
transmit-beamforming        Disable Transmit Beamforming
use                         Set setting to use
wips                        Wireless intrusion prevention related
collection                  configuration
wireless-client             Configure wireless client related parameters
wlan                        Disable a wlan from this radio
service                     Service Commands

rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#

The following example shows radio interface settings before the 'no' commands are executed:

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
    description Primary\ radio\ to\ use
    channel 1
    data-rates b-only
    mesh client
    beacon period 50
    beacon dtim-period bss 1 5
    beacon dtim-period bss 2 2
    beacon dtim-period bss 3 5
    beacon dtim-period bss 4 5
    beacon dtim-period bss 5 5
    beacon dtim-period bss 6 5
    beacon dtim-period bss 7 5
    beacon dtim-period bss 8 5
    beacon dtim-period bss 9 5
    beacon dtim-period bss 10 5
    beacon dtim-period bss 11 5
    beacon dtim-period bss 12 5
    beacon dtim-period bss 13 5
    beacon dtim-period bss 14 5
    beacon dtim-period bss 15 5
    beacon dtim-period bss 16 5
    antenna-gain 12.0
    guard-interval long
    aggregation amdu tx-only
    aeroscout forward
    ekahau forward ip 172.16.10.1 port 3
    antenna-mode 2x2
    antenna-diversity
    max-clients 100
    airt ime-fairness prefer-ht weight 6
    lock-rf-mode
    extended-range 15
antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no channel
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no antenna-gain
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no description
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no antenna-mode
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no beacon dtim-period
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#no beacon period

The following example shows radio interface settings after the ‘no’ commands are executed:

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  data-rates b-only
  mesh client
  guard-interval long
  aggregation amdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
7.1.34.4.29 non-unicast

This section describes how to configure support for forwarding of non-unicast (multicast and broadcast) frames on a radio interface.

**Supported Platforms**
- Access Points: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers: RFS4011

**Syntax**
- `non-unicast forwarding [follow-dtim|power-save-aware]`
- `non-unicast queue [<1-200>|bss <1-16> <1-200>]`
- `non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]`
- `non-unicast tx-rate bss <1-16> [dynamic-all|dynamic-basic|highest-basic|lowest-basic]`

**Parameters**
- **non-unicast forwarding**
  - Enables non-unicast frame forwarding on this radio. Once enabled, select one of the available options to specify whether these frames should always follow DTIM, or only follow DTIM when using power save aware mode.
  - **follow-dtim**: Specifies frames always wait for the DTIM interval to time out. The DTIM interval is configured using the `beacon` command. This is the default setting.
  - **power-save-aware**: Enables immediate forwarding of frames only if all associated wireless clients are in the power save mode.

- **non-unicast queue**
  - Enables non-unicast frame forwarding on this radio. Once enabled, specify the number of broadcast packets queued per BSS on this radio. This option is enabled by default. This command also enables you to override the default on a specific BSS.
  - **<1-200>**: Specify a number from 1 - 200. This value applies to all BSSs. The default is 50 frames per BSS.
  - **bss <1-16> <1-200>**: Overrides the default on a specified BSS
    - **<1-16>**: Select the BSS number from 1 - 16.
    - **<1-200>**: Specify the number of broadcast packets queued for the selected BSS from 1 - 200.

- **non-unicast tx-rate**
  - Enables non-unicast frame forwarding on this radio. Once enabled, use one of the available options to configure the rate at which these frames are transmitted.
  - **bss <1-16>**: Overrides the default on a specified BSS
    - **<1-16>**: Select the BSS number from 1 - 16. The transmit rate selected is applied only to the BSS specified here. The tx-rate options are: dynamic-all, dynamic-basic, highest-basic, lowest-basic.
  - **dynamic-all**: Dynamically selects a rate from all supported rates based on current traffic conditions.
### Examples

```bash
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#non-unicast queue bss 2 3
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#non-unicast tx-rate bss 1 dynamic-all
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
data-rates b-only
mesh client
guard-interval long
aggregation am pdu tx-only
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
non-unicast tx-rate bss 1 dynamic-all
non-unicast tx-rate bss 2 highest-basic
non-unicast tx-rate bss 3 highest-basic
non-unicast tx-rate bss 4 highest-basic
non-unicast tx-rate bss 5 highest-basic
non-unicast tx-rate bss 6 highest-basic
non-unicast tx-rate bss 7 highest-basic
non-unicast tx-rate bss 8 highest-basic
non-unicast tx-rate bss 9 highest-basic
non-unicast tx-rate bss 10 highest-basic
non-unicast tx-rate bss 11 highest-basic
non-unicast tx-rate bss 12 highest-basic
non-unicast tx-rate bss 13 highest-basic
non-unicast tx-rate bss 14 highest-basic
non-unicast tx-rate bss 15 highest-basic
non-unicast tx-rate bss 16 highest-basic
non-unicast queue bss 1 50
non-unicast queue bss 2 3
non-unicast queue bss 3 50
non-unicast queue bss 4 50
non-unicast queue bss 5 50
non-unicast queue bss 6 50
non-unicast queue bss 7 50
non-unicast queue bss 8 50
non-unicast queue bss 9 50
non-unicast queue bss 10 50
non-unicast queue bss 11 50
non-unicast queue bss 12 50
non-unicast queue bss 13 50
non-unicast queue bss 14 50
non-unicast queue bss 15 50
non-unicast queue bss 16 50
antenna-diversity
max-clients 100
airtime-fairness prefer-ht weight 6
lock-rf-mode
extended-range 15
antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Resets the handling of non-unicast frames to its default</td>
</tr>
</tbody>
</table>
7.1.34.4.30 off-channel-scan

*interface-config-radio-instance*

Enables off channel scanning on this radio. This option is disabled by default.

Channel scanning uses the access point’s resources and is time consuming. Therefore, enable this option only if the radio has the bandwidth to support channel scan without negatively impacting client support.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

- `off-channel-scan {channel-list|max-multicast|scan-interval|sniffer-redirect}`
- `off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}`
- `off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}`
- `off-channel-scan {sniffer-redirect tzsp <IP>}`

**Parameters**

- `off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| channel-list [2.4GHz|5GHz] | Optional. Selects the 2.4GHz or 5GHz access point radio band. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all channels.  
  - 2.4GHz – Selects the 2.4 GHz band  
  - 5GHz – Selects the 5.0 GHz band |
| <CHANNEL-LIST> | Optional. Specifies a list of 20 MHz, 40 MHz, or 80 MHz channels for the selected band (the channels are separated by commas or hyphens) |
| max-multicast <0-100> | Optional. Configures the maximum multicast/broadcast messages used to perform OCS  
  - <0-100> – Specify a value from 0 - 100. The default is 4. |
| scan-interval <2-100> | Optional. Configures the scan interval in dtims  
  - <2-100> – Specify a value from 2 - 100. The default is 20 dtims. |
| sniffer-redirect tzsp <IP> | Optional. Captures and redirects packets to a host running a packet capture/analysis tool. Use this command to configure the IP address of the host.  
  - tzsp – Encapsulates captured packets in TZSP before redirecting to the specified host  
  - <IP> – Specify the destination device IP address. |
Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#off-channel-scan channel-list 2.4GHz 1

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
  interface radio1
    data-rates b-only
    mesh client
      off-channel-scan channel-list 2.4GHz 1
    guard-interval long
    aggregation ampdu tx-only
    aeroscout forward
    ekahau forward ip 172.16.10.1 port 3
    non-unicast tx-rate bss 1 dynamic-all
    non-unicast tx-rate bss 2 highest-basic
    non-unicast tx-rate bss 3 highest-basic
    non-unicast tx-rate bss 4 highest-basic
    non-unicast tx-rate bss 5 highest-basic
    non-unicast tx-rate bss 6 highest-basic
    non-unicast tx-rate bss 7 highest-basic
    non-unicast tx-rate bss 8 highest-basic
    non-unicast tx-rate bss 9 highest-basic
    non-unicast tx-rate bss 10 highest-basic
    non-unicast tx-rate bss 11 highest-basic
    non-unicast tx-rate bss 12 highest-basic
    non-unicast tx-rate bss 13 highest-basic
    non-unicast tx-rate bss 14 highest-basic
    non-unicast tx-rate bss 15 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables radio off channel scanning</td>
</tr>
</tbody>
</table>
7.1.34.4.31 placement

**interface-config-radio-instance**

Defines the radio’s location (whether the radio is deployed indoors or outdoors). The radio’s placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

placement [indoor|outdoor]

**Parameters**

- placement [indoor|outdoor]

<table>
<thead>
<tr>
<th>placement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indoor</td>
<td>Radio is deployed indoors (uses indoor regulatory rules). This is the default setting.</td>
</tr>
<tr>
<td>outdoor</td>
<td>Radio is deployed outdoors (uses outdoor regulatory rules)</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#placement outdoor

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context interface radio1
data-rates b-only
placement outdoor
mesh client
off-channel-scan channel-list 2.4GHz 1
guard-interval long
aggregation ampdu tx-only
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
non-unicast tx-rate bss 1 dynamic-all
non-unicast tx-rate bss 2 highest-basic
non-unicast tx-rate bss 3 highest-basic
non-unicast tx-rate bss 4 highest-basic
non-unicast tx-rate bss 5 highest-basic
non-unicast tx-rate bss 6 highest-basic
non-unicast tx-rate bss 7 highest-basic
non-unicast tx-rate bss 8 highest-basic
non-unicast tx-rate bss 9 highest-basic
non-unicast tx-rate bss 10 highest-basic
non-unicast tx-rate bss 11 highest-basic
non-unicast tx-rate bss 12 highest-basic
non-unicast tx-rate bss 13 highest-basic
non-unicast tx-rate bss 14 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

**Related Commands**

- no | Resets a radio’s deployment location
### 7.1.34.4.32 power

#### interface-config-radio-instance

Configures the radio’s transmit power setting.

The *transmit power control* (TPC) mechanism automatically reduces the used transmission output power when other networks are within range. Reduced power results in reduced interference issues and increased battery capacity.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

#### Syntax

```
power [<1-30>|smart]
```

#### Parameters

- `power [<1-30>|smart]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>power</code></td>
<td>Configures a radio’s transmit power</td>
</tr>
<tr>
<td><code>&lt;1-30&gt;</code></td>
<td>Configures the transmit power from 1 - 30 dBm (actual power could be lower based on regulatory restrictions) For APs with dual or three radios, each radio should be configured with a unique transmit power in respect to its intended client support function.</td>
</tr>
<tr>
<td><code>smart</code></td>
<td>Enables Smart RF to determine the optimum transmit power needed. By default APs use Smart RF to determine transmit power.</td>
</tr>
</tbody>
</table>

#### Examples

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#power 12
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
    power 12
    data-rates b-only
    placement outdoor
    mesh client
    off-channel-scan channel-list 2.4GHz 1
    guard-interval long
    aggregation ampdu tx-only
    aeroscout forward
    ekahau forward ip 172.16.10.1 port 3
    non-unicast tx-rate bss 1 dynamic-all
    non-unicast tx-rate bss 2 highest-basic
    non-unicast tx-rate bss 3 highest-basic
    non-unicast tx-rate bss 4 highest-basic
    non-unicast tx-rate bss 5 highest-basic
    non-unicast tx-rate bss 6 highest-basic
    non-unicast tx-rate bss 7 highest-basic
```

--More--

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

#### Related Commands

- `no` Resets a radio’s transmit power
7.1.34.4.33 preamble-short

`interface-config-radio-instance`

Enables short preamble on this radio. If using an 802.11bg radio, enable short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

`preamble-short`

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#preamble-short
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
  interface radio1
    power 12
    data-rates b-only
    placement outdoor
    mesh client
    off-channel-scan channel-list 2.4GHz 1
    **preamble-short**
    guard-interval long
    aggregation ampdu tx-only
    aeroscout forward
    ekahau forward ip 172.16.10.1 port 3
    non-unicast tx-rate bss 1 dynamic-all
    non-unicast tx-rate bss 2 highest-basic
    non-unicast tx-rate bss 3 highest-basic
    non-unicast tx-rate bss 4 highest-basic
    non-unicast tx-rate bss 5 highest-basic
    non-unicast tx-rate bss 6 highest-basic
    non-unicast tx-rate bss 7 highest-basic
    non-unicast tx-rate bss 8 highest-basic
    non-unicast tx-rate bss 9 highest-basic
    non-unicast tx-rate bss 10 highest-basic
    non-unicast tx-rate bss 11 highest-basic
    non-unicast tx-rate bss 12 highest-basic
   --More--
  rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables the use of short preamble on a radio</td>
</tr>
</tbody>
</table>
7.1.34.4.34 probe-response

*interface-config-radio-instance*

Configures transmission parameters for probe response frames

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

probe-response [rate|retry|rssi-threshold]

- probe-response retry
- probe-response rate [follow-probe-request|highest-basic|lowest-basic]
- probe-response rssi-threshold <-128--40>

**Parameters**

- **probe-response retry**
  
  Enables retransmission of probe-response frames if no acknowledgement is received from the client. This option is enabled by default.

- **probe-response rate [follow-probe-request|highest-basic|lowest-basic]**

  
  Configures the rates used for transmission of probe response frames. The tx-rate options available for transmitting probe response frames are: follow-probe-request, highest-basic, lowest-basic.

- **follow-probe-request**

  Transmits probe responses at the same rate as the received request (default setting)

- **highest-basic**

  Uses the highest configured basic rate

- **lowest-basic**

  Uses the lowest configured basic rate

- **probe-response rssi-threshold <-128--40>**

  Ignores probe request from client if the received signal strength is less than the RSSI threshold specified here <-128--40> – Specify a value from -128 - -40.

**Examples**

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#probe-response rate highest-basic

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#probe-response retry

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#probe-response rssi-threshold -60

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#show context

interface radio1
  probe-response rate highest-basic
  probe-response rssi-threshold -60

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#

**Related Commands**

- **no**

  Resets transmission parameters for probe response frames
7.1.34.4.35 radio-resource-measurement

*interface-config-radio-instance*

Enables 802.11k radio resource measurement. When enabled, the radio station sends channel and neighbor reports.

The IEEE 802.11 Task Group k defined a set of specifications regarding radio resource measurements. These specifications specify the radio resources to be measured and the mechanism used to communicate measurement requests and results.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

**Parameters**

- `radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio-resource-measurement</td>
<td>Enables 802.11k radio resource measurement on the radio</td>
</tr>
<tr>
<td>attenuation-threshold &lt;1-199&gt;</td>
<td>Configures the neighbor attenuation threshold, considered when generating channel and neighbor reports</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-199&gt; – Specify the attenuation threshold from 1 -199. The default is 90.</td>
</tr>
<tr>
<td>max-entries &lt;1-12&gt;</td>
<td>Configures the maximum number of entries to include in channel and neighbor reports</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-12&gt; – Specify a value from 1 - 12. The default is 6.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#radio-resource-measurement attenuation-threshold 20
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#radio-resource-measurement max-entries 10
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#show context interface radio1
radio-resource-measurement max-entries 10
radio-resource-measurement attenuation-threshold 20
rfs4000-229D58(config-device-00-23-68-22-9D-587-if-radio1)#
```

**Related Commands**

- `no` Disables 802.11k radio resource measurement support
7.1.34.436 radio-share-mode

Configures the radio’s mode of operation as radio share. A radio operating in the radio share mode services clients and also performs sensor functions (defined by the radio’s AirDefense Services Platform (ADSP) licenses and profiles).

NOTE: The sensor capabilities of the radio are restricted to the channel and WLANs defined on the radio.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
radio-share-mode [inline|off|promiscuous]

Parameters
- radio-share-mode [inline|off|promiscuous]

Examples
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#radio-share-mode promiscuous

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  power 12
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  ..........................................................
  non-unicast queue bss 16 50
  antenna-diversity
  max-clients 100
  radio-share-mode promiscuous
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands
no

Resets the radio share mode for this radio to its default
7.1.34.4.37 rate-selection

Sets the rate selection method to standard or opportunistic

NOTE: This feature is not supported on RFS4011 wireless controller.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX

Syntax
rate-selection [opportunistic|standard]

Parameters
- rate-selection [opportunistic|standard]

<table>
<thead>
<tr>
<th>rate-selection</th>
<th>Sets the rate selection method to standard or opportunistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard</td>
<td>Configures the monotonic rate selection mode. This is the default setting.</td>
</tr>
<tr>
<td>opportunistic</td>
<td>Configures the opportunistic radio link adaptation (ORLA) rate selection mode</td>
</tr>
</tbody>
</table>

The ORLA algorithm is designed to select data rates that provide the best throughput. Instead of using local conditions to decide whether a data rate is acceptable or not, ORLA is designed to proactively probe other rates to determine if greater throughput is available. If these other rates do provide improved throughput, ORLA intelligently adjusts its selection tables to favour higher performance. ORLA provides improvements both on the client side of a mesh network as well as in the backhaul capabilities. ORLA is a key differentiator at the deployment and customer level and will be further explored in this paper.

Examples
nx9500-6C8809(config-profile-testAP71XX-if-radio1)#rate-selection opportunistic

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#show context
interface radio1
  rate-selection opportunistic
nx9500-6C8809(config-profile-testAP71XX-if-radio1)#

Related Commands
- no | Resets the rate selection mode to standard (monotonic)
7.1.34.4.38 rf-mode

`interface-config-radio-instance`

Configures the radio’s RF mode of operation

This command sets the mode to either 2.4 GHz WLAN or 5.0 GHz WLAN support depending on the radio’s intended client support. If you are currently licensed to use 4.9 GHz, configure the 4.9 GHz-WLAN option.

Set the mode to sensor if using the radio for rogue device detection. The radio cannot support rogue detection when one of the other radios is functioning as a WIPS sensor. To set a radio as a detector, disable sensor support on the other access point radios.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|bridge|scan-ahead|sensor]
```

**Parameters**

- `rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|bridge|scan-ahead|sensor]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rf-mode</td>
<td>Configures the radio’s RF mode of operation</td>
</tr>
<tr>
<td>2.4GHz-wlan</td>
<td>Provides WLAN service in the 2.4 GHz bandwidth</td>
</tr>
<tr>
<td>4.9GHz-wlan</td>
<td>Provides WLAN service in the 4.9 GHz bandwidth</td>
</tr>
<tr>
<td>5GHz-wlan</td>
<td>Provides WLAN service in the 5.0 GHz bandwidth</td>
</tr>
<tr>
<td>bridge</td>
<td>Enables this radio to operate as a bridge radio on 5.0 GHz bandwidth</td>
</tr>
<tr>
<td>scan-ahead</td>
<td>Enables this radio to operate as a scan-ahead radio</td>
</tr>
<tr>
<td></td>
<td>A radio functioning in the scan-ahead mode is used for forward scanning only. The radio does</td>
</tr>
<tr>
<td></td>
<td>not support WLAN or mesh services. The scan ahead feature is used in Dynamic Frequency Selection</td>
</tr>
<tr>
<td></td>
<td>(DFS) aware countries for infrastructure devices, static, and vehicular mounted modems (VMMs).</td>
</tr>
<tr>
<td></td>
<td>It enables a secondary radio to scan ahead for an active channel for backhaul transmission,</td>
</tr>
<tr>
<td></td>
<td>in the event of a radar trigger on the primary radio. The device then switches radios allowing</td>
</tr>
<tr>
<td></td>
<td>transmission to continue. This is required in environments where handoff is required and DFS</td>
</tr>
<tr>
<td></td>
<td>triggers are common.</td>
</tr>
<tr>
<td></td>
<td>With a secondary radio dedicated for forward scanning, the primary radio, in case of radar</td>
</tr>
<tr>
<td></td>
<td>hit, hands over the channel availability check (CAC) function to the secondary radio. This</td>
</tr>
<tr>
<td></td>
<td>avoids a break in data communication, which would have resulted if the primary radio was to do</td>
</tr>
<tr>
<td></td>
<td>CAC itself.</td>
</tr>
<tr>
<td></td>
<td>The secondary radio periodically does a scan of the configured channel list, searching for the</td>
</tr>
<tr>
<td></td>
<td>other available meshpoint roots. When configured on the root meshpoint, the scan-ahead feature</td>
</tr>
<tr>
<td></td>
<td>also scans for cleaner channels.</td>
</tr>
<tr>
<td>sensor</td>
<td>Operates as a sensor radio. Configures this radio to function as a scanner, providing scanning</td>
</tr>
<tr>
<td></td>
<td>services on both 2.4 GHz and 5.0 GHz bands. The radio does not provide WLAN services.</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#rf-mode sensor

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  --More--

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the radio's RF mode of operation</td>
</tr>
<tr>
<td>data-rates</td>
<td>Configures the 802.11 data rates on this radio</td>
</tr>
</tbody>
</table>
7.1.34.4.39 rifs

*interface-config-radio-instance*

Configures Reduced Interframe Spacing (RIFS) parameters on this radio

This value determines whether interframe spacing is applied to access point transmitted or received packets, both, or none. Inter-frame spacing is the interval between two consecutive Ethernet frames that enable a brief recovery between packets and allow target devices to prepare for the reception of the next packet.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

rifs [none|rx-only|tx-only|tx-rx]

**Parameters**

- **rifs [none|rx-only|tx-only|tx-rx]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Disables support for RIFS. Consider setting the value to None for high-priority traffic to reduce packet delay.</td>
</tr>
<tr>
<td>rx-only</td>
<td>Supports RIFS possession only</td>
</tr>
<tr>
<td>tx-only</td>
<td>Supports RIFS transmission only</td>
</tr>
<tr>
<td>tx-rx</td>
<td>Supports both RIFS transmission and possession (default setting)</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#rifs tx-only

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context

interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic

--More--

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

**Related Commands**

- **no** Disables radio’s RIFS parameters
### 7.1.34.4.40 rts-threshold

#### Interface-config-radio-instance

Configures the Request to Send (RTS) threshold value on this radio.

RTS is a transmitting station's signal that requests a Clear To Send (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.

The RTS threshold controls RTS/CTS by initiating an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.

Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.

A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

### Syntax

```
rts-threshold <0-65536>
```

### Parameters

- `rts-threshold <0-65536>`

### Examples

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-rad1)#rts-threshold 100
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-rad1)#show context
interface rad1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-rad1)#
```
<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Resets a radio’s RTS threshold to its default</td>
</tr>
</tbody>
</table>
7.1.34.41 service

interface-config-radio-instance

Enables dynamic control function. This dynamic function controls performance of the radio receiver's low noise amplifiers (LNAs).

When enabled, the control function, in the presence of very strong received signals, improves the receiver's performance on radio 1. Strong signals are caused if the distance between the WiFi client and the AP is within two (2) meters. When disabled, the control function is a useful debug tool in case the uplink throughput is less than expected and the AP-to-client separation is greater than two (2) meters. Disabling the control function does not affect the receive sensitivity of the radio.

Supported in the following platforms:

- Access Points — AP622, AP6522, AP6562

Syntax

```
service radio-lna [agc|ms]
```

Parameters

- service radio-lna [agc|ms]

| service radio-lna [agc|ms] | Enables dynamic control function |
|---------------------------|----------------------------------|
|                           | • agc – Enables dynamic LNA control function. This is the default setting. |
|                           | • ms – Disables dynamic LNA control function |

Examples

```
nx9500-6C8809(config-profile-testAP6522-if-radio1)#service radio-lna ms

nx9500-6C8809(config-profile-testAP6522-if-radio1)#show context interface radio1

  service radio-lna ms

nx9500-6C8809(config-profile-testAP6522-if-radio1)#
```

Related Commands

```
no
``` Reverts radio-lna mode to default (agc)
7.1.34.4.42 shutdown

*interface-config-radio-instance*

Terminates or shuts down selected radio interface

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

`shutdown`

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#shutdown
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Enables a disabled radio interface</td>
</tr>
</tbody>
</table>
7.1.34.43 smart-rf

interface-config-radio-instance

Overrides Smart RF channel width setting on this radio. When configured, the radio overrides the Smart RF selected channel setting and operates in the channel configured using this command.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP752, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

smart-rf preferred-channel-width [20MHz|40MHz|80MHz]

Parameters

smart-rf preferred-channel-width [20MHz|40MHz|80MHz]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smart-rf preferred-channel-width [2MHz</td>
<td>40MHz</td>
</tr>
<tr>
<td></td>
<td>- 20MHz – Sets 20 MHz as the preferred channel of operation</td>
</tr>
<tr>
<td></td>
<td>- 40MHz – Sets 40MHz as the preferred channel of operation</td>
</tr>
<tr>
<td></td>
<td>- 80MHz – Sets 80MHz as the preferred channel of operation (default setting)</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-profile-testAP71XX-if-radiol)#smart-rf preferred-channel-width 40MHz

nx9500-6C8809(config-profile-testAP71XX-if-radiol)#show context
interface radiol
smart-rf preferred-channel-width 40MHz
rate-selection opportunistic
nx9500-6C8809(config-profile-testAP71XX-if-radiol)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Enables use of Smart RF selected channel of operation</td>
</tr>
</tbody>
</table>
### 7.1.34.4.44 sniffer-redirect

**interface-config-radio-instance**

Captures and redirects packets to an IP address running a packet capture/analysis tool

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|10|100|100w] {snap <1-65535> (append descriptor)}
```

**Parameters**
- **sniffer-redirect [omnipeek|tzsp] <IP> channel [1|10|100|100w] {snap <1-65535> (append descriptor)}**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sniffer-redirect</td>
<td>Captures and redirects packets to an IP address running a packet capture/analysis tool</td>
</tr>
<tr>
<td>omnipeek</td>
<td>Encapsulates captured packets in proprietary header (used with OmniPeek and plug-in)</td>
</tr>
<tr>
<td>tzsp</td>
<td>Encapsulates captured packets in TZSP (used with WireShark and other tools)</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Specify the IP address of the device running the capture/analysis tool (the host to which captured off channel scan packets are redirected)</td>
</tr>
<tr>
<td>[1</td>
<td>10</td>
</tr>
<tr>
<td>• 1 – Channel 1 in 20 MHz mode (default setting)</td>
<td></td>
</tr>
<tr>
<td>• 10 – Channel 10 in 20 MHz mode</td>
<td></td>
</tr>
<tr>
<td>• 100 – Channel 100 in 20 MHz mode</td>
<td></td>
</tr>
<tr>
<td>• 100w – Channels 100w in 40 MHz mode (channels 100*,104)</td>
<td></td>
</tr>
<tr>
<td>snap &lt;1-65535&gt;</td>
<td>Optional. Allows truncating of large captured frames at a specified length (in bytes). This option is useful when capturing traffic with large frames. Use this option when only headers are needed for analysis, since it reduces the bandwidth needed for sniffing, and (for typical values) eliminates any fragmentation of the outer packet.</td>
</tr>
<tr>
<td>• &lt;1-65535&gt; – Specify the maximum truncated byte length of captured packets.</td>
<td></td>
</tr>
<tr>
<td>append descriptor</td>
<td>Optional – Enables appending of the radio’s receive descriptor to the captured packet</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#sniffer-redirect omnipeek 172.16.10.1 channel 1

rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#show context interface radiol
rf-mode sensor
placement outdoor
mesh client
rts-threshold 100
off-channel-scan channel-list 2.4GHz 1
guard-interval long
aggregation ampdu tx-only
rifs tx-only
sniffer-redirect omnipeek 172.16.10.1 channel 1
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
non-unicast tx-rate bss 1 dynamic-all
non-unicast tx-rate bss 2 highest-basic
```
non-unicast tx-rate bss 3 highest-basic
non-unicast tx-rate bss 4 highest-basic
non-unicast tx-rate bss 5 highest-basic
non-unicast tx-rate bss 6 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-rad11)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables packet capture and redirection</td>
</tr>
</tbody>
</table>
7.1.34.45 stbc

Configure the radio’s Space Time Block Coding (STBC) mode. STBC is a pre-transmission encoding scheme providing an improved SNR ratio (even at a single RF receiver). STBC transmits multiple data stream copies across multiple antennas. The receiver combines the copies into one to retrieve data from the signal. These transmitted data versions provide redundancy to increase the odds of receiving data streams with a good data decode (especially in noisy environments).

**NOTE:** STBC requires the radio has at least two antennas with the capability to transmit two streams. If the antenna mode is configured to 1x1 (or falls back to 1x1 for some reason), STBC support is automatically disabled.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**
```
stbc [auto|none|tx-only]
```

**Parameters**
- **stbc [auto|none|tx-only]**

  **stbc**
  - `auto` Autoselects STBC settings based on the platform type and other radio interface settings. This is the default setting.
  - `none` Disables STBC support
  - `tx-only` Configures the AP radio to format and broadcast the special stream (enables STBC support for transmit only)

**Examples**
```
rfs7000-37FABE(config-profile-81xxTestProfile-if-radiol)#stbc tx-only
rfs7000-37FABE(config-profile-81xxTestProfile-if-radiol)#show context interface radiol
stbc tx-only
rfs7000-37FABE(config-profile-81xxTestProfile-if-radiol)#
```

**Related Commands**
- **no** Disables STBC support
7.1.34.4.46 transmit-beamforming

Enables transmit beamforming on this radio interface. This option is disabled by default. When enabled, this option steers signals to peers in a specific direction to enhance signal strength and improve throughput amongst meshed devices (not clients). Each access point radio supports up to 16 beamforming capable mesh peers. When enabled, a beamformer steers its wireless signals to its peers. A beamformee device assists the beamformer with channel estimation by providing a feedback matrix. The feedback matrix is a set of values sent by the beamformee to assist the beamformer in computing a steering matrix. A steering matrix is an additional set of values used to steer wireless signals at the beamformer so constructive signals arrive at the beamformee for better SNR and throughput. Any beamforming capable mesh peer connecting to a radio whose capacity is exhausted cannot enable beamforming itself.

Supported in the following platforms:
- Access Points — AP8122, AP8132, AP8163

Syntax
transmit-beamforming

Parameters
None

Examples
nx9500-6C8809(config-profile-testAP81XX-if-radio1)#transmit-beamforming

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables transmit beamforming on this radio interface</td>
</tr>
</tbody>
</table>
7.1.34.4.47 use

interface-config-radio-instance

Applies an association ACL policy and a radio QoS policy on this radio interface.

An association ACL is a policy-based Access Control List (ACL) that either prevents or allows wireless clients from connecting to a controller managed access point radio. An ACL is a sequential collection of permit and deny conditions that apply to controller packets. When a packet is received on an interface, the controller compares the fields in the packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

use [association-acl-policy|radio-qos-policy]

use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy <RADIO-QOS-POLICY-NAME>]

Parameters

- use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy <RADIO-QOS-POLICY-NAME>]

<table>
<thead>
<tr>
<th>use</th>
<th>Applies an association ACL policy and a radio QoS policy on this radio interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>association-acl-policy</td>
<td>Uses a specified association ACL policy with this radio interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;ASSOC-ACL-POLICY-NAME&gt; – Specify the association ACL policy name (should be existing and fully configured).</td>
</tr>
<tr>
<td>radio-qos-policy</td>
<td>Uses a specified radio QoS policy with this radio interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;RADIO-QoS-POLICY-NAME&gt; – Specify the radio QoS policy name (should be existing and fully configured).</td>
</tr>
</tbody>
</table>

Examples

```bash
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#use association-acl-policy test

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
   rf-mode sensor
   placement outdoor
   mesh client
   rts-threshold 100
   off-channel-scan channel-list 2.4GHz 1
   guard-interval long
   aggregation ampdu tx-only
   rifs tx-only
use association-acl-policy test
sniffer-redirect omnipeek 172.16.10.1 channel 1
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
non-unicast tx-rate bss 1 dynamic-all
non-unicast tx-rate bss 2 highest-basic
non-unicast tx-rate bss 3 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Dissociates the specified association ACL policy and radio QoS policy</td>
</tr>
</tbody>
</table>
7.1.34.48 wips

`interface-config-radio-instance`

Enables access point to change its channel of operation in order to terminate rogue devices. The radio should be configured to provide WLAN service.

This option is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**NOTE:** AP7522 and AP7532 access points use Smart RF to perform off-channel scans. Therefore, ensure that a Smart RF policy is configured and applied to AP7522 and AP7532 access points RF Domains to enable them perform rogue detection and termination.

**Syntax**

`wips airtime-termination allow-channel-change`

**Parameters**

- `wips airtime-termination allow-channel-change`

| `wips airtime-termination allow-channel-change` | Enables access point to change its channel of operation (to that of the rogue device) in order to terminate the rogue device |

**Examples**

`nx9500-6C8809(config-profile-testAP81XX-if-radio1)#wips air-termination allow-channel-change`

**Related Commands**

- `no` | Disables access point to change its channel of operation in order to terminate rogue devices |
7.1.34.49 wireless-client

`interface-config-radio-instance`

Configures wireless client parameters on this radio

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

`wireless-client tx-power [<0-20>|mode]`

`wireless-client <0-20>`

`wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]`

**Parameters**

- `wireless-client tx-power <0-20>`

<table>
<thead>
<tr>
<th>wireless-client</th>
<th>Configures wireless client parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>tx-power &lt;0-20&gt;</td>
<td>Configures the transmit power indicated to wireless clients. If using a dual or three radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value.</td>
</tr>
<tr>
<td><code>&lt;0-20&gt;</code> – Specify transmit power from 0 - 20 dBm.</td>
<td></td>
</tr>
</tbody>
</table>

- `wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]`

<table>
<thead>
<tr>
<th>wireless-client</th>
<th>Configures wireless client parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>tx-power [802.11d</td>
<td>wing-ie]</td>
</tr>
<tr>
<td>802.11d – Advertises in the IEEE 802.11d country information element</td>
<td></td>
</tr>
<tr>
<td><code>wing-ie</code> – Optional. Advertises in the WiNG information element (173)</td>
<td></td>
</tr>
<tr>
<td><code>wing-ie</code> – Advertises in the WiNG information element (173). This is the default setting.</td>
<td></td>
</tr>
<tr>
<td><code>802.11d</code> – Optional. Advertises in the IEEE 802.11d country information element</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

`rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#wireless-client tx-power 20`

`rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#show context interface radiol`

`rf-mode sensor placement outdoor mesh client rts-threshold 100 wireless-client tx-power 20 off-channel-scan channel-list 2.4GHz 1 guard-interval long aggregation ampdu tx-only --More--`

`rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#`

**Related Commands**

| `no` | Resets the transmit power indicated to wireless clients |
7.1.34.450 wlan

interface-config-radio-instance

Enables a WLAN on this radio

Use this command to configure WLAN/BSS mappings for an existing access point deployment. Administrators can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:
• Access Points — AP621, AP622, AP650, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
• Wireless Controllers — RFS4011

Syntax

wlan <WLAN-NAME> {bss|primary}
wlan <WLAN-NAME> {bss <1-16>} {primary}

Parameters

• wlan <WLAN-NAME> {bss <1-16>} {primary}

| <WLAN-NAME> | Specify the WLAN name (it must have been already created and configured) |
| <bss <1-16> | primary | • bss <1-16> – Optional. Specifies a BSS for the radio to map the WLAN |
| • primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS |

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#wlan TestWLAN primary

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
rf-mode sensor
placement outdoor
mesh client
rts-threshold 100
wireless-client tx-power 20
wlan TestWLAN bss 1 primary
off-channel-scan channel-list 2.4GHz 1
guard-interval long
aggregation ampdu tx-only
rifs tx-only
use association-acl-policy test
sniffer-redirect omnipeek 172.16.10.1 channel 1
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
non-unicast tx-rate bss 1 dynamic-all
non-unicast tx-rate bss 2 highest-basic
non-unicast tx-rate bss 3 highest-basic
non-unicast tx-rate bss 4 highest-basic
non-unicast tx-rate bss 5 highest-basic
non-unicast tx-rate bss 6 highest-basic
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

no | Disables a WLAN on a radio
7.1.34.5 interface-config-wwan-instance

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a network device to connect, transmit and receive data over a cellular WAN. AP7131 model access points, RFS4000 and RFS6000 controllers utilize a PCI express card slot that supports 3G WWAN cards. The WWAN card uses *point-to-point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP establishes internet links over dial-up modems, *Digital Subscriber Line* (DSL) connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

To switch to the WWAN Interface configuration mode, use the following command:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>
```

```
rfs4000-229D58(config)#profile rfs4000 testRFS4000
```

```
rfs4000-229D58(config-profile-testRFS4000)#
```

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface wwan1
```

```
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#?
```

**Interface configuration commands:**

- **apn** Enter the access point name provided by the service provider
- **auth-type** Type of authentication, Eg chap, pap
- **crypto** Encryption Module
- **description** Port description
- **ip** Internet Protocol (IP)
- **no** Negate a command or set its defaults
- **password** Enter password provided by the service provider
- **shutdown** Disable wireless wan feature
- **use** Set setting to use
- **username** Enter username provided by the service provider
- **clrscr** Clears the display screen
- **commit** Commit all changes made in this session
- **do** Run commands from Exec mode
- **end** End current mode and change to EXEC mode
- **exit** End current mode and down to previous mode
- **help** Description of the interactive help system
- **revert** Revert changes
- **service** Service Commands
- **show** Show running system information
- **write** Write running configuration to memory or terminal

```
rfs4000-229D58(config-profile-<PROFILE-NAME>-if-wwan1)#
```

---

**NOTE:** The WWAN interface is supported only on the AP7131, RFS4000, RFS6000 platforms.

The following table summarizes WWAN interface configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>apn</strong></td>
<td>Configures the access point’s name provided by the service provider</td>
<td>page 7-299</td>
</tr>
<tr>
<td><strong>auth-type</strong></td>
<td>Configures the authentication types used on this interface</td>
<td>page 7-300</td>
</tr>
<tr>
<td><strong>crypto</strong></td>
<td>Associates a crypto map with this interface</td>
<td>page 7-301</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Associates an IP ACL with this interface</td>
<td>page 7-302</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the WWAN interface settings</td>
<td>page 7-303</td>
</tr>
<tr>
<td>password</td>
<td>Configures a password for this WWAN interface</td>
<td>page 7-304</td>
</tr>
<tr>
<td>use</td>
<td>Associates an IP ACL with this interface</td>
<td>page 7-306</td>
</tr>
<tr>
<td>username</td>
<td>Configures the names of users accessing this interface</td>
<td>page 7-307</td>
</tr>
</tbody>
</table>
7.1.34.5.1 apn

Configures the cellular data provider’s name. This setting is needed in areas with multiple cellular data providers using the same protocols, such as Europe and Asia.

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

```
apn <WORD>
```

**Parameters**

- **apn <WORD>**

  - Specify the name of the cellular data service provider.

**Examples**

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#apn AT&T

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context interface wwan1
  apn AT&T

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

**Related Commands**

- **no** Removes the configured access point name.
7.1.34.5.2 auth-type

Configure the authentication type used by the cellular data provider.

Supported platforms:
- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

Syntax
```
auth-type [chap|mschap|mschap-v2|pap]
```

Parameters
- `auth-type [chap|mschap|mschap-v2|pap]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auth-type</code></td>
<td>Configures the authentication protocol used on this interface. The options are: PAP, CHAP, MSCHAP, and MSCHAP-v2</td>
</tr>
<tr>
<td><code>chap</code></td>
<td>Configures Challenge-Handshake Authentication Protocol (CHAP). This is the default value.</td>
</tr>
<tr>
<td><code>mschap</code></td>
<td>Configures Microsoft Challenge-Handshake Authentication Protocol (MSCHAP)</td>
</tr>
<tr>
<td><code>mschapv2</code></td>
<td>Configures Microsoft Challenge-Handshake Authentication Protocol (MSCHAP) version 2</td>
</tr>
<tr>
<td><code>pap</code></td>
<td>Configures Password Authentication Protocol (PAP)</td>
</tr>
</tbody>
</table>

Examples
```bash
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#auth-type mschap-v2

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
interface wwan1
  apn AT&T
  auth-type mschap-v2
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands
```
no
```
Removes the authentication protocol configured on this interface.
7.1.34.5.3 crypto

`interface-config-wwan-instance`

Associates a crypto map with this interface

Supported in the following platforms:

- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

crypto map <CRYPTO-MAP-NAME>

**Parameters**

- crypto map <CRYPTO-MAP-NAME>

<table>
<thead>
<tr>
<th>crypto map &lt;CRYPTO-MAP-NAME&gt;</th>
<th>Associates a crypto map with this interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CRYPTO-MAP-NAME&gt;</td>
<td>- Specify the crypto map name (should be existing and configured).</td>
</tr>
</tbody>
</table>

**Examples**

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#crypto map test

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context

interface wwan1

apn AT&T

auth-type mschap-v2

`crypto map test`

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#

**Related Commands**

| no | Removes the crypto map associated with this interface |
7.1.34.5.4 ip

*interface-config-wwan-instance*

Configures IP related settings on this interface

Supported in the following platforms:

- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

\[
\text{ip } [\text{default-gateway}|\text{nat}]
\]

\[
\text{ip default-gateway priority } <1-8000>
\]

\[
\text{ip nat } [\text{inside}|\text{outside}]
\]

**Parameters**

- \text{ip default-gateway priority } <1-8000>

- \text{ip nat } [\text{inside}|\text{outside}]

**Examples**

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#ip default-gateway priority 1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#ip nat inside

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context

interface wwan1
apn AT&T
auth-type mschap-v2
crypto map test
ip nat inside
ip default-gateway priority 1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#

**Related Commands**

\text{no}

Removes IP related settings on this interface
7.1.34.5.5 no

Remove or reverts the WWAN interface settings

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

Syntax

no [all|apn|auth-type|description|ip|password|shutdown|use|username]

Usage Guidelines
The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples
The following example displays the WWAN interface settings before the ‘no’ commands are executed:

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
interface wwan1
  apn AT&T
  auth-type mschap-v2
crypto map test
  ip nat inside
  ip default-gateway priority 1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#no apn
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#no auth-type

The following example displays the WWAN interface settings after the ‘no’ commands are executed:

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
interface wwan1
crypto map test
  ip nat inside
  ip default-gateway priority 1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
7.1.34.5.6 password

*interface-config-wwan-instance*

Configures a password for this WWAN interface. The configured value is used for authentication support by the cellular data carrier.

Supported in the following platforms:
- Access Points — AP71XX
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

```
password [2 <WORD>|<WORD>]
```

**Parameters**

- `password [2 <WORD>|<WORD>]`

<table>
<thead>
<tr>
<th>password</th>
<th>Configures a password for this WWAN interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 &lt;WORD&gt;</td>
<td>Configures an encrypted password. Use this option when copy pasting the password from another device.</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>Enter the password string (should not exceed 32 characters in length).</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#password 2 TechPubsTesting@123
```

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
interface wwan1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

**Related Commands**

- `no` | Removes the configured password |
7.1.34.5.7 shutdown

interface-config-wwan-instance

Shuts down this WWAN interface. Use the no > shutdown command to re-start the WWAN interface.

Supported in the following platforms:
- Access Points — AP71XX
- Wireless Controllers — RFS4000, RFS6000

Syntax

shutdown

Parameters

None

Examples

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#shutdown

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
interface wwan1
shutdown

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Re-starts the WWAN interface</td>
</tr>
</tbody>
</table>
7.1.34.5.8 use

`interface-config-wwan-instance`

Associates an IP ACL with this interface. The ACL should be existing and configured.

The ACL applies an IP based firewall to all incoming packets. The ACL identifies a single IP or a range of IPs that are to be allowed or denied access on this interface.

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
use ip-access-list in <ACCESS-LIST-NAME>
```

Parameters

- `use ip-access-list in <ACCESS-LIST-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use ip-access-list in &lt;ACCESS-LIST-NAME&gt;</td>
<td>Associates an inbound IPv4 ACL with this interface. This setting applies to IPv4 inbound traffic only and not IPv6 traffic. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike TCP). IPv4 hosts can use link local addressing to provide local connectivity.</td>
</tr>
<tr>
<td>&lt;ACCESS-LIST-NAME&gt;</td>
<td>Specify the IP ACL name.</td>
</tr>
</tbody>
</table>

Examples

```bash
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#use ip-access-list in test

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
interface wwan1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  use ip-access-list in test
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

- `no` | Removes the IP ACL associated with this interface |
7.1.34.5.9 username

`interface-config-wwan-instance`

Configures the names of users accessing this interface
Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

`username <WORD>`

**Parameters**

- `username <WORD>`

**Examples**

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#username TechPubsUser1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context interface wwan1
   username TechPubsUser1
   password TechPubsTesting@123
   crypto map test
   ip nat inside
   use ip-access-list in test
   ip default-gateway priority 1
```

**Related Commands**

- `no` Removes the configured username
7.1.34.6 interface-config-serial-instance

This section describes the serial interface configuration commands.

Use the (config-profile-<DEVICE-PROFILE-NAME>) instance to configure the serial interface associated with the service platform.

To switch to this mode, use the following command:

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface ?

The following example uses the config-profile-default-nx45xx instance to configure a serial interface:

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface ?
WORD          Interface name
fe            Select a FastEthernet interface
ge            Select a GigabitEthernet interface
mel           Select the management interface
port-channel  Select a port channel interface
pppoe1        Select the PPP Over Ethernet interface
radio         Select a radios
serial        Select a serial interface (virtual interface)
t1e1          Select a T1 or E1 interface
up            Select the Uplink GigabitEthernet interface
vlan          Select a vlan interface (switched virtual interface)
vmif          Select the virtual interface
wwan1         Select the wireless wan interface
xge           Select a TenGigabitEthernet interface
```

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface
```

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface |serial-<1-4>/1:1|
```

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface serial-1/1:1
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#?
```

Interface configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Type of authentication, Eg chap, pap</td>
</tr>
<tr>
<td>description</td>
<td>Enter description provided by the service provider</td>
</tr>
<tr>
<td>encapsulation</td>
<td>The type of traffic that this group handles.</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>IP address assigned to the local system</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>password</td>
<td>Enter password provided by the service provider</td>
</tr>
<tr>
<td>remote-ip-subnet</td>
<td>IP subnet assigned to the remote system along with subnet in CIDR notation</td>
</tr>
<tr>
<td>remove-override</td>
<td>Remove override from the device</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disable serial interface</td>
</tr>
<tr>
<td>use</td>
<td>Set setting to use</td>
</tr>
<tr>
<td>username</td>
<td>Enter username provided by the service provider</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

```
The following table summarizes serial interface configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Configures the authentication type used on the serial interface</td>
<td>page 7-310</td>
</tr>
<tr>
<td>description</td>
<td>Configures a description of the serial interface</td>
<td>page 7-311</td>
</tr>
<tr>
<td>encapsulation</td>
<td>Defines the type of traffic handled by the serial interface</td>
<td>page 7-312</td>
</tr>
<tr>
<td>ip</td>
<td>Configures serial interface IP to use NAT</td>
<td>page 7-313</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Assigns a local IP address for this serial interface</td>
<td>page 7-314</td>
</tr>
<tr>
<td>no</td>
<td>Disables or reverts serial interface settings to their defaults</td>
<td>page 7-315</td>
</tr>
<tr>
<td>password</td>
<td>Configures the serial interface's password</td>
<td>page 7-316</td>
</tr>
<tr>
<td>remote-ip-subnet</td>
<td>Configures the remote system's IP address and subnet</td>
<td>page 7-317</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides</td>
<td>page 7-318</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the serial interface</td>
<td>page 7-320</td>
</tr>
<tr>
<td>use</td>
<td>Applies an IP access list on this serial interface</td>
<td>page 7-321</td>
</tr>
<tr>
<td>username</td>
<td>Configures the serial interface's user names</td>
<td>page 7-322</td>
</tr>
</tbody>
</table>
7.1.34.6.1 authentication

Syntax

```
interface-config-serial-instance
```

Configures the type of authentication used for this serial interface

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
authentication [chap|none|pap]
```

**Parameters**

- **authentication [chap|none|pap]**

| authentication [chap|none|pap] | Sets the type of authentication for this interface |
|-------------------------------|--------------------------------------------------|
| chap                          | Configures the authentication mode as CHAP       |
| none                          | Configures no authentication mode                |
| pap                           | Configures the authentication mode as PAP        |

**Examples**

```
x4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#authentication pap
```

```
x4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context interface serial-1/1:1 authentication pap
```

```
x4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

**Related Commands**

- **no**

  Disables or reverts serial interface settings to their default
7.1.34.6.2 description

`interface-config-serial-instance`

Configures a string that describes the serial interface (supplied by the service provider)

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

description <WORD>

**Parameters**

- description <WORD>

<table>
<thead>
<tr>
<th>description &lt;WORD&gt;</th>
<th>Configures the serial interface's description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>Provide a unique description for this serial interface (should not exceed 32 characters in length)</td>
</tr>
</tbody>
</table>

**Examples**

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#description "This interface is for the Sales Team"
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
    interface serial-1/1:1
        authentication pap
        description "This interface is for the Sales Team"
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

**Related Commands**

- `no` Removes the serial interface’s description
7.1.34.6.3 encapsulation

*interface-config-serial-instance*

Defines the data encapsulation protocol used on this serial interface

Supported in the following platforms:
  - Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

encapsulation [chdlc|ppp]

**Parameters**

- encapsulation [chdlc|ppp]

| encapsulation [chdlc|ppp] | Configures the data encapsulation protocol used |
|---------------------------|-------------------------------------------------|
| chdlc – Configures the encapsulation type as *Cisco High-Level Data Link Control* (CHDLC). CHDLC is a CISCO proprietary protocol that uses HDLC to send data over synchronous serial links. |
| ppp – Configures the encapsulation type as *Point-to-Point Protocol* (PPP) |

**Examples**

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#encapsulation chdlc

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
encapsulation chdlc
   authentication pap
   description "This interface is for the Sales Team"

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#

**Related Commands**

- no Disables or reverts serial interface settings to their default
7.1.34.6.4 ip

*interface-config-serial-instance*

Configures serial interface IP to use NAT. NAT allows for multiple devices on a LAN with private IP addresses to share a single public IP address.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

`ip nat [inside|outside]`

**Parameters**

- `ip nat [inside|outside]`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip nat</code></td>
<td>Enables the use of NAT on this serial interface</td>
</tr>
<tr>
<td><code>inside</code></td>
<td>Marks this serial interface as NAT inside interface</td>
</tr>
<tr>
<td><code>outside</code></td>
<td>Marks this serial interface as NAT outside interface</td>
</tr>
</tbody>
</table>

**Examples**

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#ip nat inside
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
interface serial-1/1:1
  encapsulation chdlc
  authentication pap
  ip nat inside
  description "This interface is for the Sales Team"
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

**Related Commands**

- `no` Disables or reverts serial interface settings to their default
### 7.1.34.6.5 local-ip-address

*interface-config-serial-instance*

Assigns a local IP address for this serial interface

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
local-ip-address <IP>
```

**Parameters**

- `local-ip-address <IP>`

**Examples**

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#local-ip-address 192.168.13.7
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
   interface serial-1/1:1
      encapsulation chdlc
      authentication pap
      local-ip-address 192.168.13.7
      ip nat inside
      description "This interface is for the Sales Team"
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

**Related Commands**

- `no` Disables or reverts serial interface settings to their default
7.1.34.6.6 no

`interface-config-serial-instance`

Removes or resets this serial interface’s settings

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
no [authentication|description|ip|local-ip-address|password|remote-ip-address|
    shutdown|use|username]
```

```
no [authentication|description|local-ip-address|password|remote-ip-address|shutdown|
    username]
```

```
no ip nat
```

```
no use ip-access-list in
```

**Parameters**

- no <PARAMETERS>

---

**Usage Guidelines**

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

**Examples**

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#no ?
authentication Type of authentication. Eg chap, pap
description Delete the description of this interface
description Delete the description of this interface
ip Internet Protocol (IP)
local-ip-address IP address assigned to the local system
password Enter password provided by the service provider
remote-ip-subnet IP subnet assigned to the remote system along with subnet
    in CIDR notation
shutdown Enable serial interface
use Set setting to use
username Enter username provided by the service provider
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```
### 7.1.34.6.7 password

**interface-config-serial-instance**

Configures the serial interface's password (supplied by the service provider)

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
password <WORD>
```

**Parameters**

- `password <WORD>`

**Examples**

````
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#password testing@1234
```

````
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
interface serial-1/1:1
   encapsulation chdlc
   authentication pap
   password testing@1234
   local-ip-address 192.168.13.7
   ip nat inside
   description "This interface is for the Sales Team"
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables or reverts serial interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.6.8 remote-ip-subnet

`interface-config-serial-instance`

Configures the remote system’s IP address and subnet in the classes inter-domain routing (CIDR) format

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```remote-ip-subnet <IP/M>```

**Parameters**

- `remote-ip-subnet <IP/M>`

| **remote-ip-subnet <IP/M>** | Defines a IP subnet assigned to the remote system along with subnet. Specify the IP address and subnet value in the A.B.C.D/M format. |

**Examples**

```nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remote-ip-subnet 192.168.0.10/24
```

```nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
interface serial-1/1:1
  encapsulation chdlc
  authentication pap
  password testing@1234
  local-ip-address 192.168.13.7
  remote-ip-subnet 192.168.13.10/24
  ip nat inside
  description "This interface is for the Sales Team"
```

**Related Commands**

- `no` Disables or reverts serial interface settings to their default
7.1.34.6.9 remove-override

Removes device overrides and applies the profile-level setting based on the parameters passed

Supported in the following platforms:
• Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

```
remove-override [authentication|description|encapsulation|ip|local-ip-address|
                    password|remote-ip-subnet|shutdown|use|username]
remove-override [authentication|description|encapsulation|local-ip-address|
                    password|remote-ip-subnet|shutdown|username]
remove-override ip nat
remove-override use ip-access-list in
```

Parameters

• remove-override <PARAMETERS>

<table>
<thead>
<tr>
<th>remove-override &lt;PARAMETERS&gt;</th>
<th>Removes serial interface related overrides applied on the device to enable profile settings to take effect</th>
</tr>
</thead>
</table>

Examples

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override ?
  authentication Remove override for authentication
  description Remove override for description
  encapsulation Remove override for encapsulation
  ip Internet Protocol (IP)
  local-ip-address Remove override for local-ip-address
  password Remove override for password
  remote-ip-subnet Remove override for remote-ip-subnet
  shutdown Remove override for serial interface
  use Set setting to use
  username Remove override for username
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override encapsulation
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override ?
  authentication Remove override for authentication
  description Remove override for description
  encapsulation Remove override for encapsulation
  ip Internet Protocol (IP)
  local-ip-address Remove override for local-ip-address
  password Remove override for password
  remote-ip-subnet Remove override for remote-ip-subnet
  shutdown Remove override for serial interface
  use Set setting to use
  username Remove override for username
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override encapsulation
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override encapsulation
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
  interface serial-1/1:1
    encapsulation chdlc
    authentication pap
    password testing@1234
    local-ip-address 192.168.13.7
    remote-ip-subnet 192.168.13.10/24
    ip nat inside
    description "This interface is for the Sales Team"
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override encapsulation
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
  interface serial-1/1:1
    authentication pap
    password testing@1234
    local-ip-address 192.168.13.7
    remote-ip-subnet 192.168.13.10/24
    ip nat inside
    description "This interface is for the Sales Team"
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#remove-override encapsulation
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
  interface serial-1/1:1
    authentication pap
    password testing@1234
    local-ip-address 192.168.13.7
    remote-ip-subnet 192.168.13.10/24
    ip nat inside
    description "This interface is for the Sales Team"
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables or reverts serial interface settings to their default</td>
</tr>
</tbody>
</table>
### 7.1.34.6.10 shutdown

Shuts down the serial interface. Use the no shutdown command to re-start a serial interface.

**Supported in the following platforms:**
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
shutdown
```

**Parameters**
None

**Examples**

```
nx4500-5CFA2B(config-profile-default-nx6500-if-serial-1/1:1)#shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables or reverts serial interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.34.6.11 use

Applies an IP access list on this serial interface

Supported in the following platforms:
  • Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

use ip-access-list in <IP-ACCESS-LIST-NAME>

Parameters

• use ip-access-list in <IP-ACCESS-LIST-NAME>

| use ip-access-list in <IP-ACCESS-LIST-NAME> | Applies an IP access list on this serial interface
|---------------------------------------------|--------------------------------------------------|
|                                             | • in – Applies the IP ACL on incoming packets
|                                             | • <IP-ACCESS-LIST-NAME> – Specify the IP access list name (it should be an existing and configured). |

Examples

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#use ip-access-list in BROADCAST-MULTICAST-CONTROL

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context interface serial-1/1:1
  authentication pap
  password testing@1234
  local-ip-address 192.168.13.7
  remote-ip-subnet 192.168.13.10/24
  ip nat inside
  use ip-access-list in BROADCAST-MULTICAST-CONTROL
description "This interface is for the Sales Team"

Related Commands

no | Disables or reverts serial interface settings to their default
### 7.1.34.6.12 username

*interface-config-serial-instance*

Configures the names of users accessing this serial interface (provided by the service provider)

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

`username <WORD>`

**Parameters**

- `username <WORD>`

<table>
<thead>
<tr>
<th>username &lt;WORD&gt;</th>
<th>Configures the user names on this serial interface. The user names are provided by the service provider, and should not exceed 32 characters in length.</th>
</tr>
</thead>
</table>

**Examples**

nx4500-5CFA2B(config-profile-default-nx6500-if-serial-1/1:1)#username SalesPerson1

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context

```
interface serial-1/1:1
  authentication pap
  username SalesPerson1
  password testing@1234
  local-ip-address 192.168.13.7
  remote-ip-subnet 192.168.13.10/24
  ip nat inside
  use ip-access-list in BROADCAST-MULTICAST-CONTROL
  description "This interface is for the Sales Team"
```

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#

**Related Commands**

| no | Disables or reverts serial interface settings to their default |
7.1.34.7 interface-config-t1e1-instance

interface

The T1/E1 interfaces are physical layer interfaces that support data, voice, or a combination of data and voice applications.

Use the (config-profile-<DEVICE-PROFILE-NAME>) instance to configure the T1E1 interface associated with the service platform.

To switch to this mode, use the following command:

<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface ?

The following example uses the config-profile-default-nx65xx instance to configure a T1E1 interface:

nx6500-31FABE(config-profile-default-nx6500)#interface t1e1 1 1
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)##

nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#?

Interface Configuration commands:

- channel-group
- clock-mode
- description
- high-impedance
- line-build-out
- line-encoding
- media
- no
- remove-override
- rx-sensitivity-level
- shutdown

nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#

The following table summarizes T1E1 interface configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group</td>
<td>Creates a channel group and assigns an index number</td>
<td>page 7-325</td>
</tr>
<tr>
<td>clock-mode</td>
<td>Configures the selected T1E1 interface's clock mode</td>
<td>page 7-326</td>
</tr>
<tr>
<td>description</td>
<td>Configures the selected T1E1 interface’s description</td>
<td>page 7-327</td>
</tr>
<tr>
<td>high-impedance</td>
<td>Enables high-impedance monitoring on the selected T1E1 interface</td>
<td>page 7-328</td>
</tr>
<tr>
<td>line-build-out</td>
<td>Defines the line build out in decibels (dB), ohms (OH), or feet (ft)</td>
<td>page 7-329</td>
</tr>
<tr>
<td>line-encoding</td>
<td>Configures the selected T1E1 interface’s encoding type</td>
<td>page 7-330</td>
</tr>
<tr>
<td>media</td>
<td>Configures the media type for the physical interface</td>
<td>page 7-331</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts T1E1 interface settings to default</td>
<td>page 7-332</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides on the selected T1E1 interface</td>
<td>page 7-333</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>rx-sensitivity-level</td>
<td>Configures the receive sensitivity level in decibels (dB)</td>
<td>page 7-334</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the selected T1E1 interface</td>
<td>page 7-335</td>
</tr>
</tbody>
</table>
7.1.34.7.1 channel-group

(interface-config-t1e1-instance)

Creates a channel group on the selected interface. Channel groups are created to provide WAN data services.

Supported in the following platforms:
  • Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

channel-group <1-1> timeslots [<TIMESLOT-LIST>|all]

Parameters

- channel-group <1-1> timeslots [<TIMESLOT-LIST>|all]

<table>
<thead>
<tr>
<th>channel-group &lt;1-1&gt;</th>
<th>Specify the channel group index</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeslots [&lt;TIMESLOT-LIST&gt;</td>
<td>all]</td>
</tr>
</tbody>
</table>
  • <TIMESLOT-LIST> – Specifies a list of timeslot IDs in the following format: 10-20, 25, 30-31
  • all – Configures all timeslots for the specified channel group

Examples

nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#channel-group 1 timeslots all
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context interface t1e1-1/1
  channel-group 1 timeslots all
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#

Related Commands

| no | Removes the channel group configured on the T1E1 interface |
7.1.34.7.2 clock-mode

`interface-config-t1e1-instance`

Configures the mode for the clock on the selected T1E1 interface. A synchronized clock mode ensures smooth clock extraction and data transfer.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```
clock-mode [master|normal]
```

**Parameters**

- `clock-mode [master|normal]`

**Examples**

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#clock-mode master
```

```
nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
channel-group 1 timeslots all
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```

**Related Commands**

- `no` Reverts the T1E1 interface clock mode to default (normal)
### 7.1.34.7.3 description

*interface-config-t1e1-instance*

Configures the selected T1E1 interface’s description

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

description <LINE>

**Parameters**

- description <LINE>

<table>
<thead>
<tr>
<th>description &lt;LINE&gt;</th>
<th>Provide a unique description for this T1E1 interface. The description should not exceed 64 characters in length and should help identify the interface.</th>
</tr>
</thead>
</table>

**Examples**

nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#description "t1 interface slot 1 Main Office"

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
channel-group 1 timeslots all
description "t1 interface slot 1 Main Office"
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#

**Related Commands**

| no | Removes or resets the T1E1 interface description |
7.1.34.7.4 high-impedance

*interface-config-t1e1-instance*

Enables high impedance monitoring on the selected T1E1 interface. High impedance interfaces imply low current and high voltage.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

`high-impedance [disable|enable]`

**Parameters**

- `high-impedance [disable|enable]`

**Examples**

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#high-impedance enable
```

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
  high-impedance enable
  channel-group 1 timeslots all
description "t1 interface slot 1 Main Office"
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```

**Related Commands**

- `no` — Resets the high impedance setting to either enable or disable
7.1.34.7.5 line-build-out

Defines the line build out in decibels (dB), ohms (OH), or feet (ft). This command specifies the distance to the next repeater.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

```
line-build-out [dB|OH|ft]
```

```
line-build-out [0-110ft|0dB|110-120ft|120OH|15dB|22.5dB|220-330ft|330-440ft|440-550ft|550-660ft|7.5dB|75OH]
```

Parameters

- line-build-out [0-110ft|0dB|110-120ft|120OH|15dB|22.5dB|220-330ft|330-440ft|440-550ft|550-660ft|7.5dB|75OH]

<table>
<thead>
<tr>
<th>line-build-out</th>
<th>Defines the line build out in decibels (dB), ohms (OH), or feet (ft)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dB</td>
<td>OH</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The valid line-build-out values for media t1 are: 0dB, 7.5dB, 15dB, 22.5dB, 0-110ft, 110-220ft, 220-330ft, 330-440ft, 440-550ft, and 550-660ft. Recommended default is 0dB.

Examples

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#line-build-out 120OH
```

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
line-build-out 120OH
high-impedance enable
channel-group 1 timeslots all
description "t1 interface slot 1 Main Office"
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```

Related Commands

```
no
```
Resets the T1/E1 interface line-build-out setting
7.1.34.7.6 line-encoding

`interface-config-t1e1-instance`

Configures the line encoding type on the selected T1E1 interface

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

```
line-encoding [ami|b8zs]
```

Parameters

- `line-encoding [ami|b8zs]`

| line-encoding [ami|b8zs] | Sets the line encoding type (designated by the service provider). The options are ami and b8zs |
|--------------------------|------------------------------------------------------------------------------------------------|
| ami                      | Configures encoding type as *Alternate Mark Inversion* (ami). This option is commonly used for the E1 interfaces. |
| b8zs                     | Configures the encoding type as *Bipolar 8-Zero Substitution* (b8zs). This option is commonly used for T1 interfaces. |

Examples

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#line-encoding ami
```

```
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context
t1e1-1/1
  clock-mode master
  line-encoding ami
  line-build-out 120OH
  high-impedance enable
  channel-group 1 timeslots all
  description "t1 interface slot 1 Main Office"
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```

Related Commands

- `no` Resets the T1E1 interface line-encoding setting
7.1.34.7.7 media

 Configures the media type for the physical interface

 Supported in the following platforms:
 - Service Platforms — NX4500, NX4524, NX6500, NX6524

 Syntax

 media [e1|t1]

 Parameters
 - media [e1|t1]

| media [e1|t1] | Sets the media type for the physical interface. The options are: e1 and t1. |
|--------------|-------------------------------------------------------------------------|
|              | • e1 – E1 (common for Europe and worldwide)                             |
|              | • t1 – T1 (common for USA and Canada)                                   |
|              | If high-impedance is set to 'enable', and media                        |

 Examples

 nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#media t1

 nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context
 interface t1e1-1/1
 clock-mode master
 line-encoding ami
 line-build-out 1200H
 high-impedance enable
 channel-group 1 timeslots all
 media t1
 description "t1 interface slot 1 Main Office"
 nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#

 Related Commands

 no | Resets the T1E1 interface media type setting |
7.1.34.7.8 no

Negates or reverts settings to default

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

no [channel-group|clock-mode|description|high-impedance|line-encoding|media|shutdown]

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes or reverts this t1e1 interface’s settings based on the parameters passed |

Examples

The following example displays the t1e1 interface settings before the 'no' commands are executed:

```bash
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
line-encoding ami
line-build-out 1200H
**high-impedance enable**
rx-sensitivity-level 30dB
channel-group 1 timeslots all
media t1
description "t1 interface slot 1 Main Office"
xn5400-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```

```bash
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#no channel-group 1
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#no high-impedance
```

The following example displays the t1e1 interface settings after the 'no' commands are executed:

```bash
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
line-encoding ami
line-build-out 1200H
**high-impedance disable**
rx-sensitivity-level 30dB
media t1
description "t1 interface slot 1 Main Office"
xn4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```
### 7.1.34.7.9 remove-override

*interface-config-t1e1-instance*

Removes device overrides on the selected T1E1 interface

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```bash
remove-override [channel-group|clock-mode|description|high-impedance|line-build-out|line-encoding|media|shutdown]
```

**Parameters**

- `remove-override` `<PARAMETERS>`

<table>
<thead>
<tr>
<th>remove-override <code>&lt;PARAMETERS&gt;</code></th>
<th>Removes device-level overrides based on the parameters passed</th>
</tr>
</thead>
</table>

**Examples**

```bash
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#remove-override ?
channel-group Channel-group for this interface
clock-mode Delete clock-mode
description Delete the description of this interface
high-impedance Delete high-impedance
line-encoding Delete line-encoding
media Delete media
shutdown Enable t1 interface
```

```bash
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#
```
7.1.34.7.10 rx-sensitivity-level

Configure the receive sensitivity level, in decibels (dB), on the selected T1E1 interface

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

rx-sensitivity-level [0dB|12dB|18dB|30dB|36dB|43dB]

Parameters

- rx-sensitivity-level [0dB|12dB|18dB|30dB|36dB|43dB]

| rx-sensitivity-level [0dB|12dB|18dB|30dB|36dB|43dB] | Sets the receive sensitivity level in decibels (dB) |
|--------------------------------------------------|--------------------------------------------------|
| [0dB|12dB|18dB|30dB|36dB|43dB]                        | • 0dB – 0 decibels                                 |
|                                                 | • 12dB – 12 decibels                               |
|                                                 | • 17.5dB – 17.5 decibels                           |
|                                                 | • 18dB – 18 decibels                               |
|                                                 | • 22.5dB – 22.5 decibels                           |
|                                                 | • 30dB – 30 decibels                               |
|                                                 | • 36dB – 36 decibels                               |
|                                                 | • 43dB – 43 decibels                               |

If high-impedance is set to ‘enable’, and media is set to either ‘t1’ or ‘e1’, the valid rx-sensitivity-level values are: 30dB and 12dB. The recommended value is 30dB.

Examples

nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#rx-sensitivity-level 30dB

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-t1e1-1/1)#show context
interface t1e1-1/1
clock-mode master
line-encoding ami
line-build-out 1200H
high-impedance enable
rx-sensitivity-level 30dB
channel-group 1 timeslots all
media t1
description "t1 interface slot 1 Main Office"
nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#

Related Commands

<table>
<thead>
<tr>
<th>no</th>
<th>Removes or resets rx sensitivity settings</th>
</tr>
</thead>
</table>
7.1.34.7.11 shutdown

- interface-config-t1e1-instance

Shuts down the selected T1E1 interface. Use the no > shutdown command to re-start the interface.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

shutdown

Parameters

None

Examples

nx4500-5CFA2B(config-profile-testNX45XX-if-t1e1-1/1)#shutdown

Related Commands

| no | Re-starts the T1E1 interface |
WiNG provides a dataplane bridge for external network connectivity for Virtual Machines (VMs). VM interfaces are layer 2 interfaces on WiNG bridge that define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two physical VM interfaces. Each VM interface can be mapped to one of eight VMIF ports for and NX4500 and NX6500 service platforms and twelve ports for NX9500 on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1 is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.

Use the (config-profile-<DEVICE-PROFILE-NAME>) instance to configure the VM interface associated with the service platform profile.

To switch to this mode, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface ?
```

The following example uses the config-profile-default-nx45xx instance to configure a VM interface:

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface vmif ?
<1-8> Interface index
```

```
nx4500-5CFA2B(config-profile-default-nx45xx)#interface vmif 2
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#?
VM Interface Mode commands:
description Port description
ip Internet Protocol (IP)
ipv6 Internet Protocol version 6 (IPv6)
no Negate a command or set its defaults
qos Quality of service
switchport Set switching mode characteristics
use Set setting to use
clsrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile-default-nx9000)#interface vmif ?
<1-12> Interface index
```

```
nx9500-6C8809(config-profile-default-nx9000)#
```
nx9500-6C8809(config-profile-default-nx9000)#interface vmif 2
nx9500-6C8809(config-profile-default-nx9000-if-vmif2)#?

VM Interface Mode commands:
- description: Configures a short description of this VM interface
- ip: Configures settings related to ARP and DHCP responses
- ipv6: Configures the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this VM interface
- no: Removes or reverts the VM interface settings
- qos: Configures the Quality of Service (QoS) settings on this VM interface
- switchport: Defines the switching mode settings for this VM interface
- use: Configures inbound IP and MAC address firewall rules for this VM interface

nx9500-6C8809(config-profile-default-nx9000-if-vmif2)#

The following table summarizes VM interface configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Configures a short description of this VM interface</td>
<td>page 7-338</td>
</tr>
<tr>
<td>ip</td>
<td>Configures settings related to ARP and DHCP responses</td>
<td>page 7-339</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this VM interface</td>
<td>page 7-340</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the VM interface settings</td>
<td>page 7-341</td>
</tr>
<tr>
<td>qos</td>
<td>Configures the Quality of Service (QoS) settings on this VM interface</td>
<td>page 7-342</td>
</tr>
<tr>
<td>switchport</td>
<td>Defines the switching mode settings for this VM interface</td>
<td>page 7-343</td>
</tr>
<tr>
<td>use</td>
<td>Configures inbound IP and MAC address firewall rules for this VM interface</td>
<td>page 7-346</td>
</tr>
</tbody>
</table>
7.1.34.8.1 description

Syntax

```
description <WORD>
```

Parameters

- `description <WORD>`

Examples

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#description "This VM interface is reserved for TEAM-URC"
```
```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context interface vmif2
    description "This VM interface is reserved for TEAM-URC"
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

Related Commands

```
no
```

Removes the description configured for this VM interface
7.1.34.8.2 ip

Configures IP settings related to ARP and DHCP responses

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

Syntax

```
ip [arp|dhcp]
ip arp [header-mismatch-validation|trust]
ip dhcp trust
```

Parameters

- ip arp [header-mismatch-validation|trust]
- ip dhcp trust

Examples

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#ip arp trust
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#ip arp header-mismatch-validation
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context interface vmif2
description "This VM interface is reserved for TEAM-URC"
ip arp trust
ip arp header-mismatch-validation
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

Related Commands

```
no
```

Disables ARP response trust and source MAC mismatch check on this VM interface. Also disables DHCP response trust setting.
7.1.34.8.3 ipv6

Sets the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this VM interface.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

Syntax

ipv6 [dhcpv6|nd]

ipv6 dhcpv6 trust

ipv6 nd [header-mismatch-validation|raguard|trust]

Parameters

- ipv6 dhcpv6 trust
  - Sets the DHCPv6 trust state for DHCPv6 responses on this VM interface. When enabled, all DHCPv6 responses received on this port are trusted and forwarded. And a DHCPv6 server can be connected only on a trusted port. This option is enabled by default.

- ipv6 nd [header-mismatch-validation|raguard|trust]
  - ipv6 nd header-mismatch-validation
    - Checks for mismatch of source MAC address in the ICMPv6 ND header and Ethernet header (link layer option). This option is disabled by default.
  - ipv6 nd raguard
    - Allows redirection of router advertisements (RAs) and ICMPv6 packets originating on this interface. Router advertisements are periodically sent either to hosts or in response to solicitation requests. The RA includes IPv6 prefixes and other subnet and host information. This option is enabled by default.
  - ipv6 nd trust
    - Sets trust state for ND requests received on this interface. When enabled, only DHCPv6 responses are trusted and forwarded on this VM interface, and a DHCPv6 server can be connected only to a trusted port. DHCPv6 relay agents receive messages from clients and forward them to a DHCPv6 server. The server sends responses back to the relay agent, and the relay agent sends the responses to the client on the local link. This option is disabled by default.

Examples

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-vmif1)#ipv6 dhcpv6 trust

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-vmif1)#ipv6 nd trust

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-vmif1)#show context interface vmif1

ipv6 dhcpv6 trust

ipv6 nd trust

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-vmif1)#

Related Commands

no
  - Removes or reverts IPv6 settings on this interface
7.1.34.8.4 no

`interface-config-vm-instance`

Removes or reverts the VM interface settings

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
no [description|ip|ipv6|qos|switchport|use]
no ip [arp|dhcp]
no ip arp [header-mismatch-validation|trust]
no ip dhcp trust

no ipv6 [dhcpv6|nd]
no ipv6 dhcpv6 trust
no ipv6 nd [header-mismatch-validation|raguard|trust]

no qos trust [802.1p|cos|dscp]

no switchport [access vlan|mode|trunk native tagged]

no use [ip-access-list|ipv6-access-list|mac-access-list] in
```

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Removes or reverts this VM interface’s settings based on the parameters passed |

**Examples**

The following example displays the VM interface settings before the ‘no’ commands are executed:

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context
interface vmif2
  description "This VM interface is reserved for TEAM-URC"
  switchport mode trunk
  switchport trunk native vlan 200
  no switchport trunk native tagged
  switchport trunk allowed vlan 200
  use ip-access-list in BROADCAST-MULTICAST-CONTROL
  ip arp trust
  ip arp header-mismatch-validation

nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

The following example displays the VM interface settings after the ‘no’ commands have been executed:

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context
interface vmif2
  switchport mode trunk
  switchport trunk native vlan 200
  no switchport trunk native tagged
  switchport trunk allowed vlan 200

nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```
7.1.34.8.5 qos

`interface-config-vm-instance`

Configures the Quality of Service (QoS) settings on this VM interface.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

### Syntax

```
qos trust [802.1p|cos|dscp]
```

### Parameters

- `qos trust [802.1p|cos|dscp]`

<table>
<thead>
<tr>
<th>qos</th>
<th>Configures the QoS settings on this VM interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>`trust [802.1p</td>
<td>cos]`</td>
</tr>
<tr>
<td><code>trust dscp</code></td>
<td>Enables trust for IP Differentiated Services Code Point (DSCP) values received on this VM interface. The option is enabled by default. DSCP values in a IP packet determines the level of service assigned to the packet.</td>
</tr>
</tbody>
</table>

### Examples

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#qos trust 802.1p
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#qos trust dscp
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#no qos trust cos
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context
interface vmif2
   switchport mode trunk
   switchport trunk native vlan 200
   no switchport trunk native tagged
   switchport trunk allowed vlan 200
   no qos trust 802.1p
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

### Related Commands

- `no` Removes QoS settings on this VM interface.
### 7.134.8.6 switchport

*interface-config-vm-instance*

Defines the switching mode settings for this VM interface

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
switchport [access|mode|trunk]
```

```
switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

```
switchport mode [access|trunk]
```

```
switchport trunk [allowed|native]
```

```
switchport trunk allowed vlan [<1-4094>|add <VLAN-ID>|none|remove <VLAN-ID>]
```

```
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

**Parameters**

- **switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]**

  Specifies the VLAN used when the switching mode is set to access. Use one of the following options to provide the VLAN ID:
  - `<1-4094>` – Specify the VLAN ID from 1 - 4094.
  - `<VLAN-ALIAS-NAME>` – Specify the VLAN alias name. The VLAN alias should be existing and mapped to the required VLAN interface.

  **Note:** use the `switchport > mode > access` command to select the access mode.

- **switchport mode [access|trunk]**

  Sets the VLAN switching mode over the VM interface. The options are: access and trunk.

- **access**

  Sets the VLAN switching mode to access. This option enables the VM interface to accept packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the VM port are expected as untagged and are mapped to the native VLAN. This is the default setting.

  If selecting access, use the `switchport > access > vlan` command to specify the VLAN interfaces used in the access mode.

- **trunk**

  Sets the VLAN switching mode to `trunk`. This option enables the VM interface to allow packets from a list of VLANs added to the trunk. A VM interface configured as trunk supports multiple 802.1Q tagged VLANs and one native VLAN. The native VLAN can be tagged or untagged.

  If selecting trunk, use the `switchport > trunk > allowed/native` command to specify the VLANs and the native VLAN.
### switchport trunk allowed vlan [1-4094]|add <VLAN-ID>|none|remove <VLAN-ID>]

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| switchport trunk allowed | Specifies the VLANs allowed when the switching mode is set to trunk.
| Specifies the list of allowed VLANs (from which packets can be accepted in the trunking mode). This command also allows the modification of an existing list. |

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan [1-4094]</td>
<td>add</td>
</tr>
<tr>
<td>1-4094 – Configures the list of VLAN IDs.</td>
<td></td>
</tr>
<tr>
<td>add &lt;VLAN-ID&gt; – Adds the VLAN ID, identified by the &lt;VLAN-ID&gt; keyword, to an existing list. Add VLANs that exclusively send packets over the VM interface. The available range is from 1 - 4094. The maximum number of entries is 256.</td>
<td></td>
</tr>
<tr>
<td>none – Removes all VLANs from an existing list.</td>
<td></td>
</tr>
<tr>
<td>remove &lt;VLAN-ID&gt; – Removes the VLAN ID, identified by the &lt;VLAN-ID&gt; keyword, from an existing list.</td>
<td></td>
</tr>
</tbody>
</table>

### switchport trunk native [tagged|vlan [1-4094]|<VLAN-ALIAS-NAME>]]

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport trunk native</td>
<td>Specifies the native VLAN allowed when the switching mode is set to trunk.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tagged</td>
<td>Select this option to tag the native VLAN.</td>
</tr>
<tr>
<td>Service Platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream VMIF that the frame belongs. If the upstream VMIF does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between VM interface ports, both VM interfaces must support tagging and be configured to accept tagged VLANs. When a frame is tagged, a 12 bit frame VLAN ID is added to the 802.1Q header, so upstream VM interfaces know which VLAN ID the frame belongs to. The 12 bit VLAN ID is read and the frame is forwarded to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VMIF classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan [1-4094]</td>
<td>&lt;VLAN-ALIAS-NAME&gt;]</td>
</tr>
<tr>
<td>Use one of the following options to provide the native VLAN ID:</td>
<td></td>
</tr>
<tr>
<td>&lt;1-4094&gt; – Specify the native VLAN ID from 1 - 4094.</td>
<td></td>
</tr>
<tr>
<td>&lt;VLAN-ALIAS-NAME&gt; – Specify the VLAN alias name. The VLAN alias should be existing and mapped to the required native VLAN interface.</td>
<td></td>
</tr>
<tr>
<td>The default native VLAN value is 1.</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

```bash
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#switchport mode trunk

nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#switchport trunk native vlan 200

nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context
interface vmif2
   description "This VM interface is reserved for TEAM-URC"
   switchport mode trunk
   switchport trunk native vlan 200
   no switchport trunk native tagged
   switchport trunk allowed vlan 200
```
ip arp trust
ip arp header-mismatch-validation
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the switching mode settings</td>
</tr>
</tbody>
</table>
7.1.34.8.7 use

Applies inbound IPv4, IPv6, and MAC specific firewall rules to this profile’s VM interface. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
use [ip-access-list|ipv6-access-list|mac-access-list] in <IP/IPv6/MAC-ACCESS-LIST-NAME>
```

**Parameters**

- `use [ip-access-list|ipv6-access-list|mac-access-list] in <IP/IPv6/MAC-ACCESS-LIST-NAME>`

| `use ip-access-list in <IP-ACCESS-LIST-NAME>` | Applies a IPv4 ACL to the inbound traffic on this VM interface. The IP ACL should be existing and configured. |
| `use ipv6-access-list in <IPv6-ACCESS-LIST-NAME>` | Applies a IPv6 ACL to the inbound traffic on this VM interface. The IPv6 ACL should be existing and configured. |
| `use mac-access-list in <MAC-ACCESS-LIST-NAME>` | Applies a MAC ACL to the inbound traffic on this VM interface. The MAC ACL should be existing and configured. |

**Examples**

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#use ip-access-list in BROADCAST-MULTICAST-CONTROL
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#show context
interface vmif2
description "This VM interface is reserved for TEAM-URC"
switchport mode trunk
switchport trunk native vlan 200
no switchport trunk native tagged
switchport trunk allowed vlan 200
use ip-access-list in BROADCAST-MULTICAST-CONTROL
ip arp trust
ip arp header-mismatch-validation
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#
```

**Related Commands**

```
no
```

Removes the IP or MAC access control list associated with this VM interface
7.1.35 *ip*

*Profile Config Commands*

The following table summarizes NAT pool configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ip</em></td>
<td>Configures IP components, such as default gateway, DHCP, DNS server forward, name server, domain name, routing standards etc.</td>
<td>page 7-348</td>
</tr>
<tr>
<td><em>nat-pool-config-instance</em></td>
<td>Invokes NAT pool configuration parameters</td>
<td>page 7-354</td>
</tr>
</tbody>
</table>
7.1.35.1  ip

ip

Configures IPv4 routing components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards etc.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`ip [default-gateway|dhcp|dns-server-forward|domain-lookup|domain-name|igmp|name-server|nat|route|routing]`

`ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcp-client <1-1800>|static-route <1-1800>]]`

`ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>|routing]`

`ip dhcp client [hostname|persistent-lease]`

`ip igmp snooping [forward-unknown-multicast|querier]`

`ip igmp snooping [forward-unknown-multicast]`

`ip igmp snooping [querier] {max-response-time <1-25>|query-interval <1-18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-3}}`

---

NOTE: The command 'ip igmp snooping' can be configured under bridge VLAN context also. For example: rfs7000-37FABE(config-device 00-15-70-37-FA-BE-bridge-vlan-1)#ip igmp snooping forward-unknown-multicast

---

`ip nat [crypto|inside|outside|pool]`

`ip nat [crypto source pool|pool] <NAT-POOL-NAME>`

`ip nat [inside|outside] [destination|source]`

`ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> <1-65535>)]`

`ip nat [inside|outside] source [list|static]`

`ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> <1-65535>)]`


`ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]`
**Parameters**

- `ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcp-client <1-1800>|static-route <1-1800>]]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Configures default gateway's IP address</td>
</tr>
<tr>
<td><code>failover</code></td>
<td>Configures failover to the gateway (with next higher priority) when the current default gateway is unreachable.</td>
</tr>
<tr>
<td><code>&lt;HOST-ALIAS-NAME&gt;</code></td>
<td>Configures the host alias mapped to the required default gateway</td>
</tr>
<tr>
<td><code>priority</code> [dhcp-client &lt;1-1800&gt;</td>
<td>static-route &lt;1-1800&gt;]</td>
</tr>
</tbody>
</table>

- `ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>|routing]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dns-server-forward</code></td>
<td>Enables DNS forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network.</td>
</tr>
<tr>
<td><code>domain-lookup</code></td>
<td>Enables domain lookup. When enabled, human friendly domain names are converted into numerical IP destination addresses.</td>
</tr>
<tr>
<td><code>domain-name &lt;DOMAIN-NAME&gt;</code></td>
<td>Configures a default domain name</td>
</tr>
<tr>
<td><code>name-server &lt;IP&gt;</code></td>
<td>Configures the name server's IP address</td>
</tr>
<tr>
<td><code>routing</code></td>
<td>Enables IP routing of logically addressed packets from their source to their destination. IPv4 routing is enabled by default.</td>
</tr>
</tbody>
</table>

- `ip dhcp client [hostname|persistent-lease]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip</code></td>
<td>Configures IPv4 routing components</td>
</tr>
</tbody>
</table>
**dhcpp**
- **Client**
  - `hostname` (optional)
    - Sets the DHCP client hostname.
  - `persistent-lease` (optional)
    - Retains the last lease across reboot if the DHCP server is unreachable.

**ip igmp snooping**
- `forward-unknown-multicast`
  - Enables unknown multicast data packets to be flooded in the specified VLAN.

**ip igmp snooping**
- `querier`
  - Enables the IGMP querier functionality for the specified VLAN.

**ip igmp snooping**
- `max-response-time <1-25>`
  - Configures the IGMP maximum query response interval used in IGMP V2/V3 queries.
- `query-interval <1-18000>`
  - Configures the IGMP querier query interval in seconds.
- `robustness-variable <1-7>`
  - Configures the IGMP robustness variable.
- `timer expiry <60-300>`
  - Configures the other querier timeout value.
- `version <1-3>`
  - Configures the IGMP query version.

**ip nat**
- `crypto source pool <NAT-POOL-NAME>`
  - Configures the NAT source address translation settings for IPSec tunnels.
- `pool <NAT-POOL-NAME>`
  - Configures a pool of IP addresses for NAT.

**ip nat**
- `inside|outside` destination static `<ACTUAL-IP> <1-65535>`
  - Configures a static NAT mapping.
### ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp] {<NATTED-IP>{<1-65535>}}
- **inside** – Configures inside address translation
- **outside** – Configures outside address translation

**destination static**
- **<ACTUAL-IP>**
- The following keywords are common to the ‘inside’ and ‘outside’ parameters:
  - destination – Specifies destination address translation parameters
  - static – Specifies static NAT local to global mapping
  - <ACTUAL-IP> – Specify the actual outside IP address to map.
- **<1-65535> [tcp|udp]**
  - <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535.
  - tcp – Configures Transmission Control Protocol (TCP) port
  - udp – Configures User Datagram Protocol (UDP) port

**<NATTED-IP> <1-65535>**
- Enables configuration of the outside natted IP address
  - <NATTED-IP> – Specify the outside natted IP address.
  - <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

### ip Configures IPv4 routing components

### nat Configures the NAT parameters

### [inside|outside] Configures inside and outside address translation for the source
- **inside** – Configures inside address translation
- **outside** – Configures outside address translation

**source static**
- **<ACTUAL-IP>**
- The following keywords are common to the ‘inside’ and ‘outside’ parameters:
  - source – Specifies source address translation parameters
  - static – Specifies static NAT local to global mapping
  - <ACTUAL-IP> – Specify the actual inside IP address to map.
- **<1-65535> [tcp|udp]**
  - <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535.
  - tcp – Configures Transmission Control Protocol (TCP) port
  - udp – Configures User Datagram Protocol (UDP) port

**<NATTED-IP> <1-65535>**
- Enables configuration of the outside natted IP address
  - <NATTED-IP> – Specify the outside natted IP address.
  - <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

- Configures an access list describing local addresses
  - <IP-ACCESS-LIST-NAME> – Specify a name for the IP access list.
ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#ip default-gateway 172.16.10.4
rfs7000-37FABE(config-profile-default-rfs7000)#ip dns-server-forward
rfs7000-37FABE(config-profile-default-rfs7000)#ip nat inside source list test interface vlan 1 pool pool1 overload

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
    bridging-mode isolated-tunnel
    ip igmp snooping querier
    ip default-gateway 172.16.10.4
    autoinstall configuration
    autoinstall firmware
    crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
    crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  gos trust 802.1p
  interface ge3
    ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge4
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface pppoe1
use firewall-policy default
ip dns-server-forward
ip nat inside source list test interface vlan1 pool pooll overload
service pm sys-restart
router ospf

rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#?
Nat Policy Mode commands:
   address Specify addresses for the nat pool
   no      Negate a command or set its defaults
   clrscr  Clears the display screen
   commit  Commit all changes made in this session
   do      Run commands from Exec mode
   end     End current mode and change to EXEC mode
   exit    End current mode and down to previous mode
   help    Description of the interactive help system
   revert  Revert changes
   service Service Commands
   show    Show running system information
   write   Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)

Related Commands

|   no   | Disables or reverts settings to their default |
7.1.35.2 nat-pool-config-instance

Use the config-profile-<DEVICE-PROFILE-NAME> instance to configure Network Address Translation (NAT) pool settings.

The following example uses the config-profile-default-rfs7000 instance to configure NAT pool settings:

```
rfs7000-37FABE(config-profile-default-rfs7000)#ip nat pool pool1
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#?
```

Nat Policy Mode commands:
- address: Specify addresses for the nat pool
- no: Negate a command or set its defaults
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)
```

The following table summarizes NAT pool configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Configures NAT pool addresses</td>
<td>page 7-355</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 7-356</td>
</tr>
</tbody>
</table>
### 7.1.35.2.1 address

* `<nat-pool-config-instance>`

Configures NAT pool of IP addresses

Define a range of IP addresses hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
address [<IP>|range <START-IP> <END-IP>]
```

#### Parameters

- **address [<IP>|range <START-IP> <END-IP>]]**

<table>
<thead>
<tr>
<th><strong>Parameters</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Adds a single IP address to the NAT pool</td>
</tr>
<tr>
<td>range</td>
<td>Adds a range of IP addresses to the NAT pool</td>
</tr>
<tr>
<td>&lt;START-IP&gt;</td>
<td>Specify the starting IP address of the range.</td>
</tr>
<tr>
<td>&lt;END-IP&gt;</td>
<td>Specify the ending IP address of the range.</td>
</tr>
</tbody>
</table>

#### Examples

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#address range 172.16.10.2 172.16.10.8
```

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#show context ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#
```

#### Related Commands

- `no` | Removes address(es) configured with this NAT pool |
7.1.35.2.2 no

- nat-pool-config-instance

Removes address(es) configured with this NAT pool

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
no address [<IP>|range <START-IP> <END-IP>]

Parameters
- no address [<IP>|range <START-IP> <END-IP>]

| no address [<IP>| | range <START-IP> <END-IP>] | Removes a single IP address or a range of IP addresses from this NAT pool |

Usage Guidelines
The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#show context
   ip nat pool pool1
       address range 172.16.10.2 172.16.10.8
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#no address range 172.16.10.2 172.16.10.8
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#

Related Commands

| address | Configures NAT pool IP address(es) |
7.1.36 ipv6

Profile Config Commands

Configures IPv6 routing components, such as default gateway, DNS server forwarding, name server, routing standards etc.

These IPv6 settings are applied to all devices using this profile.

You can also configure IPv6 settings on a device, using the device’s configuration mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

NOTE: The IPv6 settings configured at the profile/device level are global configuration settings and not interface-specific.

Syntax

```
ipv6 [default-gateway|dns-server-forward|hop-limit|mld|name-server|nd-reachable-time|
neighbor|ns-interval|ra-convert|route|ula-reject-route|unicast-routing]
```

```
ipv6 [default-gateway <IPv6> {vlan <VLAN-ID>}|
dns-server-forward|hop-limit <1-255>|
name-server <IPv6>|nd-reachable-time <5000-3600000>|ns-interval <1000-3600000>|
ula-reject-route|unicast-routing]
```

```
ipv6 ra-convert {throttle interval <3-1800> max-RAs <1-256>}
```

```
ipv6 mld snooping {forward-unknown-multicast|querier}
```

```
ipv6 mld snooping {forward-unknown-multicast}
```

```
ipv6 mld snooping {querier} {max-response-time <1-25000>|query-interval <1-18000>|
robustness-variable <1-7>|timer expiry <60-300>|version <1-2>}
```

```
ipv6 neighbor [<IPv6>|timeout]
```

```
ipv6 neighbor <IPv6> <MAC> [<INTF-NAME]|pppo1|vlan <1-4094>|wwan1] {dhcp-server|
router}
```

```
ipv6 neighbor timeout <15-86400>
```

```
ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-ID>}
```

Parameters

- ipv6 [default-gateway <IPv6> {vlan <VLAN-ID>}|dns-server-forward|hop-limit <1-255>|
nname-server <IPv6>|nd-reachable-time <5000-3600000>|ns-interval <1000-3600000>|
ula-reject-route|unicast-routing]

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Configures IPv6 routing components</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-gateway &lt;IPv6&gt; {vlan &lt;VLAN-ID&gt;}</td>
<td>Configures IPv6 default gateway's address in the ::/0 format</td>
</tr>
<tr>
<td>dns-server-forward</td>
<td>Enables DNS server forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network. This feature is disabled by default.</td>
</tr>
<tr>
<td>hop-limit &lt;1-255&gt;</td>
<td>Configures the IPv6 hop count limit</td>
</tr>
</tbody>
</table>

- <1-255> – Specify a value between 1 - 255. The default is 64.
**name-server <IPv6>**
Configures the IPv6 name server's address
- `<IPv6>` – Specify the address of the IPv6 name server.

**nd-reachable-time <5000-3600000>**
Configures the time, in milliseconds, that a neighbor is assumed to be reachable after having received neighbor discovery (ND) confirmation for their reachability
- `<5000-3600000>` – Specify a value from 5000 - 3600000 milliseconds. The default is 30,000 milliseconds.

**ns-interval <1000-3600000>**
Configures the interval, in milliseconds, between two consecutive retransmitted neighbor solicitation (NS) messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address.
- `<1000-3600000>` – Specify a value from 1000 - 3600000. The default is 1000 milliseconds.

**ula-reject-route**
Installs a "reject" route for Unique Local Address (ULA) prefixes. This ensures that site-border routers and firewalls do not forward packets with ULA source or destination addresses outside of the site, unless explicitly configured with routing information about specific /48 or longer Local IPv6 prefixes. This option is disabled by default.
The ULA is an IPv6 address used in private networks for local communication within a site (for example a company, campus, or within a set of branch office networks). These site local addresses are IPv6 addresses that fall in the block fc00::/7, defined in RFC 4193.

**unicast-routing**
Enables IPv6 unicast routing. This feature is enabled by default.

- `ipv6 ra-convert { throttle interval <3-1800> max-RAs <1-256> }`

**ipv6**
Configures IPv6 routing components

**ra-convert { throttle interval <3-1800> max-RAs <1-256> }**
Enables conversion of multicast router advertisements (RAs) to unicast RAs at the dot11 layer. This feature is disabled by default.
- `throttle` – Optional. Throttles multicast RAs before converting to unicast
  - `interval <3-1800>` – Throttles multicast RAs for a specified time period. Specify the interval from 3 - 1800 seconds. The default is 3 seconds.
  - `max-RAs <1-256>` – Specifies the maximum number of RAs per IPv6 router during the specified throttle interval. Specify a value from 1 - 256. The default is 1.

- `ipv6 mld snooping { forward-unknown-multicast }`

**ipv6**
Configures IPv6 routing components

**mld snooping forward-unknown-multicast**
Enables *multicast listener discovery* (MLD) protocol snooping. This feature is disabled by default.
When enabled, IPv6 devices (access point, wireless controller, or service platform) can examine MLD messages exchanged between hosts and multicast routers to discern which hosts are receiving multicast group traffic. Based on the information gathered these devices forward multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces. This prevents VLANs from getting flooded with IPv6 multicast traffic.
- `forward-unknown-multicast` – Optional. Enables unknown multicast forwarding. This feature is enabled by default.
- ipv6 mld snooping \{querier\} \{max-response-time <1-25000>|query-interval <1-18000>| robustness-variable <1-7>|timer expiry <60-300>|version <1-2}\}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Configures IPv6 routing components</td>
</tr>
<tr>
<td>mld snooping querier</td>
<td>Enables MLD protocol snooping</td>
</tr>
<tr>
<td>querier</td>
<td>• querier – Optional. Enables the on-board MLD querier. When enabled, IPv6 devices send query messages to discover which network devices are members of a given multicast group. This option is disabled by default.</td>
</tr>
<tr>
<td>max-response-time &lt;1-25000&gt;</td>
<td>Configures the MLD querier’s maximum query response time. This is the time for which the querier waits before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic.</td>
</tr>
<tr>
<td>query-interval &lt;1-18000&gt;</td>
<td>Configures the interval, in seconds, between two consecutive MLD querier’s queries. The robustness variable is an indication of how susceptible the subnet is to lost packets. MLD can recover from robustness variable minus 1 lost MLD packets.</td>
</tr>
<tr>
<td>robustness-variable &lt;1-7&gt;</td>
<td>Configures the MLD IGMP robustness variable. This value is used by the sender of a query.</td>
</tr>
<tr>
<td>timer expiry &lt;60-300&gt;</td>
<td>Configures the MLD other querier (any external querier) timeout</td>
</tr>
<tr>
<td>version &lt;1-2&gt;</td>
<td>Configures the MLD querier’s version. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2.</td>
</tr>
</tbody>
</table>

- ipv6 neighbor <IPv6> <MAC> \{<INTF-NAME>|pppoel|vlan <1-4094>|wwan1\} \{dhcp-server| router\}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Configures IPv6 routing components</td>
</tr>
<tr>
<td>neighbor</td>
<td>Configures static IPv6 neighbor entries</td>
</tr>
<tr>
<td>&lt;IPv6&gt;</td>
<td>Specify the IPv6 address for which a static neighbor entry is created.</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Specify the MAC address associated with the specified IPv6 address.</td>
</tr>
<tr>
<td>[&lt;INTF-NAME&gt;]</td>
<td>pppoe1</td>
</tr>
<tr>
<td></td>
<td>• &lt;INTF-NAME&gt; – Selects the layer 3 router interface. Specify the interface name.</td>
</tr>
<tr>
<td></td>
<td>• pppoe1 – Selects the PPP over Ethernet interface</td>
</tr>
<tr>
<td></td>
<td>• vlan &lt;1-4094&gt; – Selects the VLAN interface. Specify the VLAN interface index.</td>
</tr>
<tr>
<td></td>
<td>• wwan1 – Selects the wireless WAN interface</td>
</tr>
<tr>
<td>{dhcp-server</td>
<td>router}</td>
</tr>
<tr>
<td></td>
<td>• dhcp-server – Optional. States this neighbor entry is for a DHCP server</td>
</tr>
<tr>
<td></td>
<td>• router – Optional. States this neighbor entry is for a router</td>
</tr>
</tbody>
</table>
• `ipv6 neighbor timeout <15-86400>`

<table>
<thead>
<tr>
<th>neighbor</th>
<th>Configures static IPv6 neighbor entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout &lt;15-86400&gt;</td>
<td>Configures the timeout, in seconds, for the static neighbor entries</td>
</tr>
<tr>
<td>• &lt;15-86400&gt;</td>
<td>Specify a value from 15 - 86400 seconds. The default is 3600 seconds.</td>
</tr>
</tbody>
</table>

• `ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-ID}>`

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Configures IPv6 routing components</th>
</tr>
</thead>
<tbody>
<tr>
<td>route</td>
<td>Configures the static routes</td>
</tr>
<tr>
<td>These routes are maintained in the IPv6 <code>Forwarding Information Base</code> (FIB).</td>
<td></td>
</tr>
<tr>
<td>Note: To view FIB6 routing entries, use the <code>service &gt; show fib6 &gt; &lt;TABLE-ID&gt;</code> command.</td>
<td></td>
</tr>
<tr>
<td>&lt;DEST-IPv6-PREFIX/PREFIX-LENGTH&gt;</td>
<td>Specify the IPv6 destination prefix (IPv6 network) and the prefix length.</td>
</tr>
<tr>
<td>&lt;IPv6-GATEWAY-ADDRESS&gt;</td>
<td>Specify the IPv6 gateway's address.</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Optional. specify the VLAN interface’s ID (through which the default gateway is accessible)</td>
</tr>
<tr>
<td>Note: This parameter is needed only if the gateway address is a link local address.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-6DCD4B(config-profile-TestRFS7000)#ipv6 default-gateway 2001:10:10:10:10:10:10:2
rfs7000-6DCD4B(config-profile-TestRFS7000)#ipv6 dns-server-forward
rfs7000-6DCD4B(config-profile-TestRFS7000)#ipv6 mld snooping
rfs7000-6DCD4B(config-profile-TestRFS7000)#show context profile rfs7000 TestRFS7000
  ipv6 mld snooping
  ipv6 dns-server-forward
  ipv6 default-gateway 2001:10:10:10:10:10:10:2
  no autoinstall configuration
  no autoinstall firmware
  crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  --More--
rfs7000-6DCD4B(config-profile-TestRFS7000)#
```

**Related Commands**

| no | Disables or reverts IPv6 settings to their default |
**7.1.37 l2tpv3**

> Profile Config Commands

Defines the L2TPv3 settings for tunneling layer 2 payloads using VPNs.

L2TPv3 is an IETF standard that defines the control and encapsulation protocol settings for tunneling layer 2 frames in an IP network (and access point profile) between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables WiNG supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between WiNG devices and other vendor devices supporting the L2TPv3 protocol.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|logging|manual-session|router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port <1024-65535>]
l2tpv3 logging ip-address [<IP>|any] hostname [<HOSTNAME>|any]
router-id [<IP>|<WORD>|any]
```

**Parameters**

- **l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|manual-session|router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port <1024-65535>]**

<table>
<thead>
<tr>
<th>l2tpv3</th>
<th>Configures the L2TPv3 protocol settings for a profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname &lt;HOSTNAME&gt;</td>
<td>Configures the host name sent in the L2TPv3 signalling messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.</td>
</tr>
<tr>
<td>inter-tunnel-bridging</td>
<td>Enables inter tunnel bridging of packets. This feature is disabled by default.</td>
</tr>
<tr>
<td>manual-session</td>
<td>Creates/modifies L2TPv3 manual sessions</td>
</tr>
<tr>
<td>For more information, see l2tpv3-manual-session-commands.</td>
<td></td>
</tr>
<tr>
<td>router-id [&lt;1-4294967295&gt;</td>
<td>&lt;IP&gt;]</td>
</tr>
<tr>
<td>- &lt;1-4294967295&gt; – Configures the router ID in decimal format from 1 - 4294967295</td>
<td></td>
</tr>
<tr>
<td>- &lt;IP&gt; – Configures the router ID in the IP address (A.B.C.D) format</td>
<td></td>
</tr>
<tr>
<td>tunnel</td>
<td>Creates/modifies a L2TPv3 tunnel</td>
</tr>
<tr>
<td>For more information, see l2tpv3-tunnel-commands.</td>
<td></td>
</tr>
<tr>
<td>udp-listen-port &lt;1024-65535&gt;</td>
<td>Configures the UDP port used to listen for incoming traffic</td>
</tr>
<tr>
<td>- &lt;1024-65535&gt; – Specify the UDP port from 1024 - 65535 (default is 1701)</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Configures L2TPv3 protocol settings for a profile</td>
</tr>
<tr>
<td>logging</td>
<td>Enables L2TPv3 tunnel event logging and debugging. When enabled, all events relating to Ethernet frames to and from bridge VLANs and physical ports on a specified IP address, host or router ID are logged. This option is disabled by default.</td>
</tr>
<tr>
<td>ip-address [&lt;IP&gt;</td>
<td>any]</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP&gt; – Specify the peer’s IP address. L2TPv3 events are captured and logged for the specified peer.</td>
</tr>
<tr>
<td></td>
<td>• any – Peer’s IP address is not specified. Enables event logging for all incoming connections from any IP address.</td>
</tr>
<tr>
<td>hostname [&lt;HOSTNAME&gt;</td>
<td>any]</td>
</tr>
<tr>
<td></td>
<td>• &lt;HOSTNAME&gt; – Specify the peer’s host name. L2TPv3 events are captured and logged for specified host.</td>
</tr>
<tr>
<td></td>
<td>• any – Peer’s hostname is not specified. Enables debugging for all incoming connections from any host.</td>
</tr>
<tr>
<td>router-id [&lt;IP&gt;</td>
<td>&lt;WORD&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP&gt; – Specify the router ID in the IP address format.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the router ID in the form of an integer or range. For example 100-200.</td>
</tr>
<tr>
<td></td>
<td>• any – Router ID is not specified. Enables debugging for all incoming connections from any L2TPv3 router.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 hostname l2tpv3Host1

rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 inter-tunnel-bridging

rfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000
  bridge vlan 1
    bridging-mode isolated-tunnel
    ip igmp snooping
    ip igmp snooping querier
  ........................................................... l2tpv3 hostname l2tpv3Host1
  l2tpv3 inter-tunnel-bridging
rfs7000-37FABE(config-profile-default-rfs7000)#

**Related Commands**

no
  Negates a L2TPv3 tunnel settings on this profile
### 7.1.38 l3e-lite-table

**Profile Config Commands**

Configures L3e lite table aging time

The L3e Lite table stores information about destinations and their location within a specific IPSec tunnel. This enables quicker packet transmissions. The table is updated as nodes transmit packets.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
l3e-lite-table aging-time <10-1000000>
```

**Parameters**

- `l3e-lite-table aging-time <10-1000000>`

<table>
<thead>
<tr>
<th>l3e-lite-table aging-time &lt;10-1000000&gt;</th>
<th>Configures the aging time in seconds. The aging time defines the duration a learned L3e entry (IP, VLAN) remains in the L3e Lite table before deletion due to lack of activity. The default is 300 seconds.</th>
</tr>
</thead>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000)#l3e-lite-table aging-time 1000
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  ..........................................................
  interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  interface pppoe1
  use firewall-policy default
l3e-lite-table aging-time 1000
  --More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

- `no`  
  Removes the L3e lite table aging time configuration
Profile Config Commands

Turns on and off access point LEDs

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`led {flash-pattern}`

Parameters

- `led {flash-pattern}`: Optional. Enables LED flashing on the device using this profile

Examples

rfs7000-37FABE(config-profile-RFS7000Test)#led flash-pattern

rfs7000-37FABE(config-profile-RFS7000Test)#show context profile rfs7000 RFS7000Test
no autoinstall configuration
no autoinstall firmware
led flash-pattern
crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-VPN
crypto ikev2 remote-VPN
crypto auto-ipsec-secure
--More--
rfs7000-37FABE(config-profile-RFS7000Test)#

Related Commands

`no` | Disables or reverts settings to their default
7.1.40 led-timeout

Profile Config Commands

Configures the LED-timeout timer in the device or profile configuration mode

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

led-timeout [<15-1440>|shutdown]

Parameters

- led-timeout [<15-1440>|shutdown]

| led-time [<15-1440>|shutdown] | Sets the LED-timeout timer. The value provided here determines the interval (time to lapse) for which a device's LEDs are turned off after the last radio state change. For example, if set at 15 minutes, the LEDs are turned off for 15 minutes after the last radio state change.
|-----------------|---------------------------------------------------------------|
| • <15-1440> – Specify a value from 15 - 1400 minutes. The default is 30 minutes.
| • shutdown – Shuts down the LED-timeout timer. The device LEDs are not turned off.

Examples

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout 25

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
  use profile default-nx9000
  use rf-domain default
  hostname nx9500-6C8809
  license AAP
  66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356al
  license HTANLT
  66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3ddee7967f30e49e497
  no autogen-uniqueid
  ip default-gateway 192.168.13.2
  led-timeout 25
  --More--

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout shutdown

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
  use profile default-nx9000
  use rf-domain default
  hostname nx9500-6C8809
  license AAP
  66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356al
  license HTANLT
  66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3ddee7967f30e49e497
  no autogen-uniqueid
  ip default-gateway 192.168.13.2
  led-timeout shutdown
  crypto ikev2 peer IKEV2Peerl
  --More--

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables LED-timeout timer</td>
</tr>
</tbody>
</table>
### 7.1.41 legacy-auto-downgrade

#### Profile Config Commands

Enables device firmware to auto downgrade when legacy devices are detected

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

legacy-auto-downgrade

#### Parameters

None

#### Examples

rfs7000-37FABE(config-profile-default-rfs7000)#legacy-auto-downgrade

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Prevents device firmware from auto downgrading when legacy devices are detected</td>
</tr>
</tbody>
</table>
7.1.42 legacy-auto-update

Profile Config Commands

Auto updates an AP650 or AP71XX legacy access point firmware

Supported in the following platforms:
- Access Points — AP650, AP7131

Syntax

legacy-auto-update [ap650|ap71xx image <FILE>]

Parameters

- legacy-auto-update [ap650|ap71xx image <FILE>]

<table>
<thead>
<tr>
<th>legacy-auto-update</th>
<th>Updates a legacy AP650 or AP7131 access point firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap650</td>
<td>Auto updates legacy AP650 firmware</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Auto updates legacy AP7131 firmware</td>
</tr>
<tr>
<td>image &lt;FILE&gt;</td>
<td>Auto updates legacy AP7131 firmware</td>
</tr>
<tr>
<td></td>
<td>• image – Sets the path to the firmware image</td>
</tr>
<tr>
<td></td>
<td>• &lt;FILE&gt; – Specify the path and filename in the flash:/ap.img format.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#legacy-auto-update ap71xx image flash:/ap47d.img

Related Commands

| no                | Disables automatic legacy firmware upgrade               |
7.1.43 lldp

Profile Config Commands

Enables LLDP on this profile and configures LLDP settings

LLDP or IEEE 802.1AB is a vendor-neutral Data Link Layer protocol used by network devices for advertising of (announcing) identity, capabilities, and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery. Both LLDP snooping and ability to generate and transmit LLDP packets is provided.

Information obtained via CDP and LLDP snooping is available in the UI. Information obtained using LLDP is provided during the adoption process, so the layer 2 device detected by the access point can be used as a criteria in the provisioning policy.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

lldp [holdtime|med-tlv-select|run|timer]

lldp [holdtime <10-1800>|run|timer <5-900>]

lldp med-tlv-select [inventory-management|power-management {auto}]

Parameters

- **lldp [holdtime <10-1800>|run|timer <5-900>]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp</td>
<td>Enables LLDP on this profile and configures LLDP settings</td>
</tr>
<tr>
<td>holdtime &lt;10-1800&gt;</td>
<td>Sets the holdtime for transmitted LLDP PDUs. This command specifies the time a receiving device holds information before discarding.</td>
</tr>
<tr>
<td>run</td>
<td>Enables LLDP on this profile</td>
</tr>
<tr>
<td>timer &lt;5-900&gt;</td>
<td>Sets the transmit interval. This command specifies the transmission frequency of LLDP updates in seconds.</td>
</tr>
</tbody>
</table>

- **lldp med-tlv-select [inventory-management|power-management {auto}]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>med-tlv-select [inventory-management</td>
<td>power-management {auto}]</td>
</tr>
<tr>
<td>inventory-management</td>
<td>Enables inventory management discovery. Allows an endpoint to convey detailed inventory information about itself. This information includes details, such as manufacturer, model, and software version etc. This option is enabled by default.</td>
</tr>
<tr>
<td>power-management auto</td>
<td>Enables extended power via MDI discovery. Allows endpoints to convey power information, such as how the device is powered, power priority etc.</td>
</tr>
<tr>
<td>auto</td>
<td>Optional. Assigns default value based on device type</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-profile-default-rfs7000)#lldp timer 20
rfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000
  bridge vlan 1
  use firewall-policy default
  ip dns-server-forward
  ip nat pool pool1
    address range 172.16.10.2 172.16.10.8
  ip nat inside source list test interface vlan1 pool pool1 overload
  lldp timer 20
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

| no                                      | Disables LLDP on this profile |
7.1.44 load-balancing

Profile Config Commands

Configures load balancing parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

load-balancing [advanced-params|balance-ap-loads|balance-band-loads|balance-channel-loads|band-control-strategy|band-ratio|group-id|neighbor-selection-strategy]


load-balancing advanced-params [2.4GHz-load|5GHz-load] [client-weightage|throughput-weightage] <0-100>
load-balancing advanced-params equality-margin [2.4GHz|5GHz] <0-100>
load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|channel-5GHz] <0-100>
load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHz] <0-100>
load-balancing advanced-params [max-neighbors <0-16>|min-common-clients <0-256>|min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]

load-balancing [balance-ap-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]

load-balancing band-control-strategy [distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]

load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]

load-balancing group-id <GROUP-ID>

load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification|use-smart-rf]

Parameters

- load-balancing advanced-params [2.4GHz-load|5GHz-load] [ap-load] [client-weightage|throughput-weightage] <0-100>

<table>
<thead>
<tr>
<th>load-balancing advanced-params</th>
<th>Configures advanced load balancing parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz-load [client-weightage</td>
<td>throughput-weightage] &lt;0-100&gt;</td>
</tr>
<tr>
<td></td>
<td>• client-weightage – Specifies weightage assigned to the client-count when calculating the 2.4 GHz load</td>
</tr>
<tr>
<td></td>
<td>• throughput-weightage – Specifies weightage assigned to throughput, when calculating the 2.4 GHz load</td>
</tr>
<tr>
<td></td>
<td>The following keyword is common to the ‘client-weightage’ and ‘throughput-weightage’ parameters:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-100&gt; – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.</td>
</tr>
</tbody>
</table>
### 5GHz-load

**[client-weightage|throughput-weightage]**  
<0-100>

<table>
<thead>
<tr>
<th>Configures 5.0 GHz load calculation weightages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• client-weightage – Specifies weightage assigned to the client-count when calculating the 5.0 GHz load</td>
</tr>
<tr>
<td>• throughput-weightage – Specifies weightage assigned to throughput, when calculating the 5.0 GHz load</td>
</tr>
</tbody>
</table>

The following keyword is common to the ‘client-weightage’ and ‘throughput-weightage’ parameters:  
• <0-100> – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.

### ap-load

**[client-weightage|throughput-weightage]**  
<0-100>

<table>
<thead>
<tr>
<th>Configures AP load calculation weightages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• client-weightage – Specifies weightage assigned to the client-count, when calculating the AP load</td>
</tr>
<tr>
<td>• throughput-weightage – Specifies weightage assigned to throughput, when calculating the AP load</td>
</tr>
</tbody>
</table>

The following keyword is common to the ‘client-weightage’ and ‘throughput-weightage’ parameters:  
• <0-100> – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.

### load-balancing

**[load-balancing advanced-params]**  
Configures advanced load balancing parameters

<table>
<thead>
<tr>
<th><strong>load-balancing advanced-params</strong></th>
</tr>
</thead>
</table>
| **equality-margin**  
[2.4GHz|5GHz|ap|band]  
<0-100>  |

<table>
<thead>
<tr>
<th>Configures the maximum load difference considered equal. The load is compared for different 2.4 GHz channels, 5.0 GHz channels, APs, or bands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2.4GHz – Configures the maximum load difference considered equal when comparing loads on different 2.4 GHz channels</td>
</tr>
<tr>
<td>• 5GHz – Configures the maximum load difference considered equal when comparing loads on different 5.0 GHz channels</td>
</tr>
<tr>
<td>• ap – Configures the maximum load difference considered equal when comparing loads on different APs</td>
</tr>
<tr>
<td>• band – Configures the maximum load difference considered equal when comparing loads on different bands</td>
</tr>
</tbody>
</table>

The following keyword is common to 2.4 GHz channels, 5.0 GHz channels, APs, and bands:  
• <0-100> – Sets the margin as a load percentage from 1 - 100. The default equality-margin for 2.5 GHz, 5.0 GHz, ap, and band loads is 1%.

### load-balancing advanced-params

<table>
<thead>
<tr>
<th>Configures advanced load balancing parameters</th>
</tr>
</thead>
</table>
| **hiwater-threshold**  
[ap|channel-2.4GHz|channel-5GHz]  
<0-100>  |

<table>
<thead>
<tr>
<th>Configures advanced load balancing parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>load-balancing advanced-params</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| **hiwater-threshold**  
[ap|channel-2.4GHz|channel-5GHz]  
<0-100>  |
### hiwater-threshold
Configures the load beyond which load balancing is invoked

| [ap|channel-2.4GHz|channel-5GHz] <0-100> | Select one of the following options: |
|-----------------------------------------|--------------------------------------|
| • ap – Configures the AP load beyond which load balancing begins |
| • channel-2.4GHz – Configures the AP load beyond which load balancing begins (for APs on 2.4 GHz channel) |
| • channel-5GHz – Configures the AP load beyond which load balancing begins for APs on 5.0 GHz channel |

The following keyword is common for the 'AP', 'channel-2.4GHz', and 'channel-5GHz' parameters:

• <0-100> – Sets the load threshold as a number from 1 - 100. The default hiwater-threshold for channel-2.5GHz, channel-5GHz, and ap loads is 5.

---

### load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHz] <0-100>
Configures advanced load balancing parameters

| max-preferred-band-load [2.4GHz|5GHz] <0-100> | Select one of the following options: |
|-----------------------------------------------|--------------------------------------|
| • 2.4GHz – Configures the maximum load on 2.4 GHz, when it is the preferred band |
| • 5GHz – Configures the maximum load on 5.0 GHz, when it is the preferred band |

The following keyword is common to the 2.4 GHz and 5.0 GHz bands:

• <0-100> – Configures the maximum load as a percentage from 0 - 100. The default value for 2.4GHz and 5.0GHz is 75%

---

### load-balancing advanced-params max-neighbors <0-16>
Configures the maximum number of confirmed neighbors to balance

<table>
<thead>
<tr>
<th>max-neighbors &lt;0-16&gt;</th>
<th>Configures the maximum number of confirmed neighbors to balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;0-16&gt; – Specify a value from 0 - 16. Optionally configure a minimum of 0 neighbors and a maximum of 16 neighbors. The default is 16.</td>
<td></td>
</tr>
</tbody>
</table>

---

### load-balancing advanced-params min-common-clients <0-256>
Configures the minimum number of common clients that can be shared with the neighbor for load balancing

<table>
<thead>
<tr>
<th>min-common-clients &lt;0-256&gt;</th>
<th>Configures the minimum number of common clients that can be shared with the neighbor for load balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;0-256&gt; – Specify a value from 0 - 256. Optionally configure a minimum of 0 clients and a maximum of 256 clients. The default is 0.</td>
<td></td>
</tr>
</tbody>
</table>

---

### load-balancing advanced-params min-neighbor-rssi <-100-30>
Configures the minimum signal strength (RSSI) of a neighbor detected

<table>
<thead>
<tr>
<th>min-neighbor-rssi &lt;-100-30&gt;</th>
<th>Configures the minimum signal strength (RSSI) of a neighbor detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;-100-30&gt; – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -65 dBm.</td>
<td></td>
</tr>
</tbody>
</table>

---

### load-balancing advanced-params min-probe-rssi <-100-30>
Configures the minimum received probe signal strength required to qualify the sender as a common client

<table>
<thead>
<tr>
<th>min-probe-rssi &lt;-100-30&gt;</th>
<th>Configures the minimum received probe signal strength required to qualify the sender as a common client</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;-100-30&gt; – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -100 dBm.</td>
<td></td>
</tr>
</tbody>
</table>
• **load-balancing** [balance-ap-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]

<table>
<thead>
<tr>
<th>load-balancing</th>
<th>Configures the following load balancing parameters: ap-loads, band-loads, and channel-loads.</th>
</tr>
</thead>
<tbody>
<tr>
<td>balance-ap-loads</td>
<td>Enables neighbor AP load balancing. This option distributes the access point's radio load amongst other controller managed access point radios. This option is disabled by default.</td>
</tr>
<tr>
<td>balance-band-loads</td>
<td>Enables balancing of the total band load amongst neighbors. This option balances the access point's radio load by assigning a ratio to both the 2.4 GHz and 5.0 GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 GHz or 5.0 GHz band. This option is disabled by default.</td>
</tr>
</tbody>
</table>
| balance-channel-loads [2.4GHz|5GHz] | Enables the following:  
  • 2.4GHz – Channel load balancing on 2.4 GHz band. This option is disabled by default. Balances the access point’s 2.4 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 2.4 GHz radio if a channel is over utilized.  
  • 5GHz – Channel load balancing on 5.0 GHz band. This option is disabled by default. Balances the access point’s 5.0 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 5.0 GHz radio if a channel is over utilized. |

• **load-balancing band-control-strategy** [distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]

| load-balancing band-control-strategy | Configures a band control strategy  
By default, this option steers 5.0 GHz-capable clients to the 5.0 GHz band. When an access point hears a request from a client to associate on both the 2.4 GHz and 5.0 GHz bands, it knows the client is capable of operation in 5.0 GHz. Band steering steers the client by responding only to the 5.0 GHz association request and not the 2.4 GHz request. Consequently, the client only associates in the 5.0 GHz band. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>distribute-by-ratio</td>
<td>Distributes clients to either band according to the band-ratio</td>
</tr>
<tr>
<td>prefer-2.4GHz</td>
<td>Nudges all dual-band clients to 2.4 GHz band</td>
</tr>
<tr>
<td>prefer-5GHz</td>
<td>Nudges all dual-band clients to 5.0 GHz band. This is the default setting.</td>
</tr>
</tbody>
</table>

• **load-balancing band-ratio [2.4GHz|5GHz] [0]<1-10>

| load-balancing band-ratio | Configures the relative loading of 2.4 GHz band and 5.0 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz or the radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz or 5.0 GHz radio band.  
2.4GHz [0]<1-10>] | Configures the relative loading of 2.4 GHz band  
  • 0 – Selecting ‘0’ steers all dual-band clients preferentially to the other band  
  • <0-10> – Configures a relative load as a number from 0 - 10. The default is 0. |
| ------ | -------------------------------------------------|
| 5ghz [0]<1-10>] | Configures the relative loading of 5.0 GHz band  
  • 0 – Selecting ‘0’ steers all dual-band clients preferentially to the other band  
  • <0-10> – Configures a relative load as a number from 0 - 10. The default is 1. |
### load-balancing group-id <GROUP-ID>

| group-id <GROUP-ID> | Configures group ID to facilitate load balancing  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;GROUP-ID&gt; – Specify the group ID. This option is enabled only when a group ID is configured.</td>
</tr>
</tbody>
</table>

### load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification| use-smart-rf]

| load-balancing neighbor-selection-strategy | Configures a neighbor selection strategy. The options are: use-common-clients, use-roam-notification, and use-smart-rf  
|-------------------------------------------|--------------------------------------------------|
| use-common-clients | Selects neighbors based on probes from clients common to neighbors. This option is enabled by default.  
| use-roam-notification | Selects neighbors based on roam notifications from roamed clients. This option is enabled by default.  
| use-smart-rf | Selects neighbors detected by Smart RF. This option is enabled by default. |

### Examples

```bash
rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing advanced-params 2.4ghz-load throughput-weightage 90
rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing advanced-params hiwater-threshold ap 90
rfs7000-37FABE(config-profile-default-rfs7000)#load-balancing balance-ap-loads
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  ip default-gateway 172.16.10.4
  autoinstall configuration
  autoinstall firmware
  load-balancing advanced-params 2.4ghz-load throughput-weightage 90
  load-balancing advanced-params hiwater-threshold ap 90
  load-balancing balance-ap-loads
  --More--
rfs7000-37FABE(config-profile-default-rfs7000)#s
```

### Related Commands

| no | Disables load balancing on this profile |
### 7.1.45 logging

*Profile Config Commands*

Enables message logging and configures logging settings. When enabled, the profile logs individual system events to a user-defined log file or a syslog server. Message logging is disabled by default.

Enabling message logging is recommended, because system event logs can be analyzed to determine an overall pattern that may be negatively impacting performance.

This command can also be executed in the device configuration mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

logging [aggregation-time|buffered|console|facility|forward|host|on|syslog]

logging [aggregation-time <1-60>|host [<IPv4>|<IPv6>]|on]

logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical|errors|warnings|notifications|informational|debugging]

logging facility [local0|local1|local2|local3|local4|local5|local6|local7]

**Parameters**

- **logging [aggregation-time <1-60>|host [<IPv4>|<IPv6>]|on]**
  - **aggregation-time <1-60>**
    - Sets the number of seconds for aggregating repeated messages. This is the interval at which system events are logged on behalf of this profile. The shorter the interval, the sooner the event is logged.
    - • <1-60> – Specify a value from 1 - 60 seconds. The default value is 0.
  - **host [<IPv4>|<IPv6>]**
    - Configures a remote host to receive log messages. Defines numerical (non DNS) IPv4 or IPv6 addresses for external resources where logged system events can be sent on behalf of the controller profile. A maximum of four entries can be made.
    - • <IPv4> – Specify the IPv4 address of the remote host.
    - • <IPv6> – Specify the IPv6 address of the remote host.

- **on**
  - Enables the logging of system messages

- **logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical|errors|warnings|notifications|informational|debugging]**
  - Enables message logging and configures logging settings

- **logging buffered**
  - Sets the buffered logging level

- **logging console**
  - Sets the console logging level

- **logging syslog**
  - Sets the syslog server’s logging level
### logging facility [local0|local1|local2|local3|local4|local5|local6|local7]

<table>
<thead>
<tr>
<th>forward</th>
<th>Forwards system debug messages to the wireless controller or service platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0-7]</td>
<td>The following keywords are common to the buffered, console, syslog, and forward parameters. All incoming messages have different severity levels based on their importance. The severity level is fixed on a scale of 0 - 7.</td>
</tr>
<tr>
<td>emergencies</td>
<td>Severity level 0: System is unusable</td>
</tr>
<tr>
<td>critical</td>
<td>Severity level 1: Requires immediate action</td>
</tr>
<tr>
<td>errors</td>
<td>Severity level 2: Critical conditions</td>
</tr>
<tr>
<td>warnings</td>
<td>Severity level 3: Error conditions</td>
</tr>
<tr>
<td>notifications</td>
<td>Severity level 4: Warning conditions (default)</td>
</tr>
<tr>
<td>informational</td>
<td>Severity level 5: Normal but significant conditions</td>
</tr>
<tr>
<td>debugging</td>
<td>Severity level 6: Informational messages</td>
</tr>
<tr>
<td>&lt;0-7&gt;</td>
<td>Sets the message logging severity level on a scale of 0 - 7</td>
</tr>
</tbody>
</table>

#### Examples

```bash
rfs7000-37FABE(config-profile-default-rfs7000)#logging facility local4
rfs7000-37FABE(config-profile-default-rfs7000)#show context
```

<table>
<thead>
<tr>
<th>service pm sys-restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>12tpv3 hostname 12tpv3Host1</td>
</tr>
<tr>
<td>12tpv3 inter-tunnel-bridging</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
</tr>
</tbody>
</table>
**7.1.46 mac-address-table**

▲ **Profile Config Commands**

Configures the MAC address table. Use this command to create MAC address table entries by assigning a static address to the MAC address table.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

mac-address-table [aging-time|static]
mac-address-table aging-time [0|<10-1000000>]
mac-address-table static <MAC> vlan <1-4094> interface [L2-INTERFACE|ge <1-4]|port-channel <1-2>

**Parameters**

- **mac-address-table aging-time [0|<10-1000000>]**
  - Sets the duration a learned MAC address persists after the last update
    - 0 – Entering the value ‘0’ disables the aging time
    - <10-1000000> – Sets the aging time from 10 - 1000000 seconds. The default is 300 seconds.

- **mac-address-table static <MAC> vlan <1-4094> interface [L2-INTERFACE|ge <1-4]|port-channel <1-2>**
  - Creates a static MAC address table entry
    - <MAC> – Specifies the static address to add to the MAC address table. Specify the MAC address in the AA-BB-CC-DD-EE-FF, AA:BB:CC:DD:EE:FF, or AABB:CC:DD:EE:FF format.

  - **vlan <1-4094>**
    - Assigns a static MAC address to a specified VLAN port
      - <1-4094> – Specify the VLAN index from 1 - 4094.

  - **interface [L2-INTERFACE]|ge <1-4]|port-channel <1-2>**
    - Specifies the interface type. The options are: layer 2 Interface, GigabitEthernet interface, and a port channel interface
      - <L2-INTERFACE> – Specify the layer 2 interface name.
      - ge – Specifies a GigabitEthernet interface
        - <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
      - port-channel – Specifies a port channel interface
        - <1-2> – Specify the port channel interface index from 1 - 2.

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000)#mac-address-table static 00-40-96-B0-BA-2A vlan 1 interface ge 1

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  .........................................................
  logging facility local4
  mac-address-table static 00-40-96-B0-BA-2A vlan 1 interface gel
  ip nat pool pool1
  --More--
  rfs7000-37FABE(config-profile-default-rfs7000)#
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables or reverts settings to their default</td>
</tr>
</tbody>
</table>
### 7.1.47 mac-auth

#### Profile Config Commands

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.</td>
</tr>
<tr>
<td>a.</td>
<td>Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.</td>
</tr>
<tr>
<td>b.</td>
<td>Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.</td>
</tr>
</tbody>
</table>

Attaching the AAA policy to the device or profile. When attached to a profile, the AAA policy is applied to all devices using this profile.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Attach the AAA policy to the device or profile. When attached to a profile, the AAA policy is applied to all devices using this profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Enable mac-auth on the device's desired GE port. When enabled on a profile, MAC address authentication is enabled, on the specified GE port, of all devices using this profile.</td>
</tr>
</tbody>
</table>
Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000

### Syntax

mac-auth use aaa-policy `<AAA-POLICY-NAME>`

### Parameters

- `mac-auth use aaa-policy `<AAA-POLICY-NAME>``

### Examples

The following examples demonstrate the configuration of authentication of MAC addresses on wired ports:

```
rfs4000-229D58 (config-aaa-policy-mac-auth)#authentication server 1 onboard controller
```

```
rfs4000-229D58 (config-aaa-policy-mac-auth)#show context
aaa-policy mac-auth
```

```
rfs4000-229D58 (config)#radius-group RG
```

```
rfs4000-229D58 (config)#radius-user-pool-policy RUG
```

```
rfs4000-229D58 (config)#radius-server-policy RS
```

```
rfs4000-229D58 (config-device-00-23-68-22-9D-58-if-ge4)#show context
interface ge4
dot1x authenticator host-mode single-host
dot1x authenticator port-control auto
```

**mac-auth** Enables 802.1X authentication of MAC addresses on this profile. Use the device configuration mode to enable this feature on a device.

**use aaa-policy `<AAA-POLICY-NAME>`** Associates an existing AAA policy with this profile (or device)

- `<AAA-POLICY NAME>` – Specify the AAA policy name.

The AAA policy used should be created especially for MAC authentication.
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
interface ge5
  switchport mode access
  switchport access vlan 1
  dot1x authenticator host-mode single-host
  dot1x authenticator guest-vlan 5
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 4
Mac Auth info for interface GE4
-----------------------------------
  Mac Auth Enabled
  Mac Auth Authorized
  Client MAC 00-16-41-55-F8-5D

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 5
Mac Auth info for interface GE5
-----------------------------------
  Mac Auth Enabled
  Mac Auth Not Authorized

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Enables authentication of MAC addresses on wired ports settings on this profile (or device)</td>
</tr>
</tbody>
</table>
7.1.48 memory-profile

Profile Config Commands

Configures memory profile used on the device

Supported in the following platforms:
  • Access Points — AP621, AP6511, AP6521

Syntax

memory-profile [adopted|standalone]

Parameters

• memory-profile [adopted|standalone]

<table>
<thead>
<tr>
<th>memory-profile</th>
<th>Configures memory profile used on the device</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopted</td>
<td>Configures adopted mode (no GUI and higher MiNT routes, firewall flows)</td>
</tr>
<tr>
<td>standalone</td>
<td>Configures standalone mode (GUI and fewer MiNT routes, firewall flows)</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-profile-testAP6511)#memory-profile adopted
Note: memory-profile change will take effect after device reboot
nx9500-6C8809(config-profile-testAP6511)#

Related Commands

no | Resets device's memory profile configuration


7.1.49 *meshpoint-device*

*Profile Config Commands*

Configures meshpoint device parameters. This feature is configurable in the profile and device configuration modes.

Supported in the following platforms:
- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX

**Syntax**

```plaintext
meshpoint-device <MESHPOINT-NAME>
```

**Parameters**

- `meshpoint-device <MESHPOINT-NAME>`

<table>
<thead>
<tr>
<th>meshpoint-device &lt;MESHPOINT-NAME&gt;</th>
<th>Configures meshpoint device parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;MESHPOINT-NAME&gt; — Specify meshpoint name.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For *Vehicular Mounted Modem* (VMM) access points or other mobile devices, set the path selection method as mobile-snr-leaf in the config-meshpoint-device mode. For more information, see `path-method`.

**Examples**

```plaintext
rfs7000-37FABE(config-profile-testAP71XX)#meshpoint-device test
rfs7000-37FABE(config-profile-testAP71XX-meshpoint-test)#?
Mesh Point Device Mode commands:
acs          Configure auto channel selection parameters
exclude      Exclude neighboring Mesh Devices
hysteresis   Configure path selection SNR hysteresis values
monitor      Event Monitoring
no           Negate a command or set its defaults
path-method  Path selection method used to find a root node
preferred    Configure preferred path parameters
root         Set this meshpoint as root
root-select  Root selection method parameters
clearscr     Clears the display screen
commit       Commit all changes made in this session
do           Run commands from Exec mode
end          End current mode and change to EXEC mode
exit         End current mode and down to previous mode
help         Description of the interactive help system
revert       Revert changes
service      Service Commands
show         Show running system information
write        Write running configuration to memory or terminal
```

```plaintext
rfs7000-37FABE(config-profile-testAP71XX-meshpoint-test)#
```

**Related Commands**

| no | Removes a specified meshpoint |

---

**NOTE:** For more information on the meshpoint-device configuration parameters, see *Chapter 26, MESHPOINT.*
7.1.50 meshpoint-monitor-interval

Profile Config Commands

Configures the meshpoint monitoring interval. This is the interval, in seconds, at which the meshpoint status is checked.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

meshpoint-monitor-interval <1-65535>

Parameters

- meshpoint-monitor-interval <1-65535>

<table>
<thead>
<tr>
<th>meshpoint-monitor-interval &lt;1-65535&gt;</th>
<th>Configures the meshpoint monitoring interval in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>– Specify the interval from 1 - 65535 seconds. The default is 30 seconds.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#meshpoint-monitor-interval 100

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  meshpoint-monitor-interval 100
  ip default-gateway 172.16.10.4
  --More--

Related Commands

| no | Resets the meshpoint monitoring interval to default (30 seconds) |
7.1.51 min-misconfiguration-recovery-time

Profile Config Commands

Configures the minimum device connectivity verification time

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

min-misconfiguration-recovery-time <60-3600>

Parameters

- min-misconfiguration-recovery-time <60-3600>

| min-misconfiguration-recovery-time <60-3600> | Configures the minimum connectivity (with the associated device) verification interval
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60-3600&gt;</td>
<td>– Specify a value from 60 - 3600 seconds (default is 60 seconds).</td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-profile-testRFS4000)#min-misconfiguration-recovery-time 500

nx9500-6C8809(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
meshpoint-monitor-interval 300
no autoinstall configuration
no autoinstall firmware
crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
    crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radiol
interface radio2
interface up1
interface ge1
interface ge2
interface ge3
interface ge4
interface ge5
interface wwan1
interface pppoe1
use firewall-policy default
min-misconfiguration-recovery-time 500
service pm sys-restart
router ospf
router bgp
nx9500-6C8809(config-profile-testRFS4000)#

Related Commands

| no | Resets setting to default (60 seconds) |
7.1.52 mint

Profile Config Commands

Configures MiNT protocol parameters required for MiNT creation and adoption

MiNT links are required for adoption of a device (APs, wireless controller, and service platform) to a controller. The MiNT link is created on both the adoptee and the adopter. WiNG provides several commands to configure MiNT links and establish adoption for both IPv4 and IPv6 addresses.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

mint [dis|level|link|mlcp|rate-limit|spf-latency|tunnel-across-extended-vlan|tunnel-controller-load-balancing]

mint dis [priority-adjustment <255-255>|strict-evis-reachability]

mint level 1 area-id <1-16777215>

mint link [force|ip|listen|vlan]


mint link [listen ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>]|vlan <1-4094>]

{adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|
ipsec-security {gw [<IP]|<HOST-NAME>]|level [1/2]}

mint link ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>]

{<1-65535>|adjacency-hold-time <2-600>|
cost <1-10000>|hello-interval <1-120>|ipsec-security {gw [<IP]|<HOST-NAME>]|level [1/2]}

mint mlcp [ip|ipv6|vlan]

mint rate-limit level2 [link|mlcp]

mint rate-limit level2 [link [ip [<IPv4>|<IPv6>]] <1-65535]|vlan <1-4094>]

mlcp [ip|ipv6|vlan] rate <50-1000000> max-burst-size <2-1024>

{red-threshold [background|best-effort|video|voice] <0-100>}

mint spf-latency <0-60>

mint tunnel-across-extended-vlan

mint tunnel-controller-load-balancing level1

Parameters

- mint dis [priority-adjustment <255-255>|strict-evis-reachability]
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **dis priority-adjustment** | Sets the relative priority for the router to become DIS (designated router)  
- priority-adjustment – Sets priority adjustment added to base priority  
The *Designated IS* (DIS) priority adjustment is the value added to the base level DIS priority to influence the DIS election. A value of +1 or greater increases DISiness.  
- <-255-255> – Specify a value from -255 - 255. The default is 0.  
**Note:** Higher numbers result in higher priorities |
| **strict-evis-reachability** | Enables reaching *Ethernet Virtualization Interconnect* (EVIS) election winners through MiNT. This option is enabled by default. |
| **mint level 1 area-id <1-16777215>** | Configures MiNT protocol parameters required for MiNT creation and adoption  
- level 1 – Configures local MiNT routing settings  
- area-id <1-16777215> – Specifies the level 1 routing area identifier  
- level 2 – Configures level 2 inter-site MiNT routing  
- adjacency-hold-time <2-600> – Specifies the adjacency lifetime after hello packets cease  
- cost <1-100000> – Specifies the link cost in arbitrary units  
- hello-interval <1-120> – Specifies the interval, in seconds, between successive hello packets  
- ipsec-security {gw [<IP>|<HOST-NAME>]} – Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.  
- gw [<IP>|<HOSTNAME>] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway’s numerical IP address or administrator defined hostname. |
| **link force ip [<IPv4>|<IPv6>][<1-65535> level 2|level 2] {adjacency-hold-time <2-600>|cost <1-100000> hello-interval <1-120> ipsec-security {gw [<IP>|<HOST-NAME>]}** | Configures MiNT protocol parameters required for MiNT creation and adoption  
- link force – Creates a MiNT routing link as a forced link  
- force – Forces a MiNT routing link to be created even if not necessary  
- ip [<IPv4>|<IPv6>] – Creates a MiNT tunnel over UDP/IPv4 or IPv6  
- Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MiNT protocol.  
- <IPv4> – Specify the MiNT tunnel peer’s IPv4 address.  
- <IPv6> – Specify the MiNT tunnel peer’s IPv6 address.  
- After specifying the MiNT peer’s address, configure the following MiNT link parameters: UDP port, adjacency-hold-time, cost, hello-interval, IPSec security gateway, and routing level.  
- <1-65535> level 2 – Optional. Specifies a custom UDP port for MiNT links. Specify the port from 1 - 65535.  
- adjacency-hold-time <2-600> – Optional. Specifies the adjacency lifetime after hello packets cease  
- cost <1-100000> – Optional. Specifies the link cost in arbitrary units  
- hello-interval <1-120> – Optional. Specifies the interval, in seconds, between successive hello packets  
- ipsec-security {gw [<IP>|<HOST-NAME>]} – Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.  
- gw [<IP>|<HOSTNAME>] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway’s numerical IP address or administrator defined hostname. |
### mint

<table>
<thead>
<tr>
<th>mint</th>
<th>Configures MiNT protocol parameters required for MiNT creation and adoption</th>
</tr>
</thead>
</table>

#### mint listen ip

- **listen ip**
- 
  - `{<IPv4>|<IPv6>|<HOST-ALIAS-NAME>}`
- **adjacency-hold-time**
  - `<2-600>`
- **cost**
  - `<1-10000>`
- **hello-interval**
  - `<1-120>`
- **level**
  - `[1|2]`
- **ipsec-security**
  - `{gw `{<IP>|<HOST-NAME>}`}`

- **mint listen ip**
- 
  - `{<IPv4>|<IPv6>|<HOST-ALIAS-NAME>}`
  - Creates a MiNT routing link
  - • listen – Creates a MiNT listening link
    - • ip – Creates a MiNT listening link over UDP/IP or IPv6
      - • `<IPv4>` – Specify the IPv4 address of the listening UDP/IP link.
      - • `<IPv6>` – Specify the IPv6 address of the listening UDP/IP link.
      - • `<HOST-ALIAS-NAME>` – Specify the host alias identifying the MiNT link address. The host alias should existing and configured.

- **UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted. The typical configuration is to have a listening UDP/IP link on the IP address S.S.S.S, and for all the APs to have a regular UDP/IP link to S.S.S.S.**

#### link vlan <1-4094>

- **link vlan**
- 
  - `<1-4094>`
  - Enables MiNT routing on VLAN
  - • vlan – Defines a VLAN ID used by peers for inter-operation when supporting the MiNT protocol.
    - • `<1-4094>` – Select VLAN ID from 1 - 4094.

- **adjacency-hold-time**
- 
  - `<2-600>`
  - This parameter is common to the ‘listen’ and ‘vlan’ parameters:
    - • adjacency-hold-time `<2-600>` – Optional. Specifies the adjacency lifetime after hello packets cease
    - • `<2-600>` – Specify a value from 2 - 600 seconds. The default is 46 seconds.

  **Note:** For MiNT VLAN routing the default is 13 seconds.

- **cost `<1-100000>`**
- 
  - `<1-100000>`
  - This parameter is common to the ‘listen’ and ‘vlan’ parameters:
    - • cost `<1-100000>` – Optional. Specifies the link cost in arbitrary units
      - • `<1-100000>` – Specify a value from 1 - 100000. The default is 100.

  **Note:** For MiNT VLAN routing the default is 10.

- **hello-interval `<1-120>`**
- 
  - `<1-120>`
  - This parameter is common to the ‘listen’ and ‘vlan’ parameters:
    - • hello-interval `<1-120>` – Optional. Specifies the interval, in seconds, between successive hello packets
      - • `<1-120>` – Specify a value from 1 - 120. The default is 15 seconds.

  **Note:** For MiNT VLAN routing the default is 4 seconds.

- **level `[1|2]`**
- 
  - `[1|2]`
  - This parameter is common to the ‘listen’ and ‘vlan’ parameters:
    - Optional. Specifies the routing levels for this routing link. The options are:
      - • 1 – Configures local routing
      - • 2 – Configures inter-site routing

- **ipsec-security `{gw `{<IP>|<HOST-NAME>}`}`**
- 
  - `{gw `{<IP>|<HOST-NAME>}`}`
  - This parameter is common to the ‘listen’ and ‘vlan’ parameters:
    - • ipsec-security – Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.
      - • gw `{<IP>|<HOSTNAME>}` – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway’s numerical IP address or administrator defined hostname.
  Selects the peer UDP port from 1 - 65535.

- `adjacency-hold-time <2-600>`
  Optional. Specifies the adjacency lifetime after hello packets cease.  
  `<2-600>` – Specify a value from 2 - 600 seconds. The default is 46 seconds.

- `cost <1-10000>`
  Optional. Specifies the link cost in arbitrary units.  
  `<1-10000>` – Specify a value from 1 - 100000. The default is 100.

- `hello-interval <1-120>`
  Optional. Specifies the interval, in seconds, between successive hello packets.  
  `<1-120>` – Specify a value from 1 - 120. The default is 15 seconds.

- `level [1|2]`
  Optional. Specifies the routing levels for this routing link. The options are:  
  • 1 – Configures local routing  
  • 2 – Configures inter-site routing

- `ipsec-security {gw [IP]<HOST-NAME>]}
  Optional. Enables IPSec secure peer authentication on the MiNT connection (link).  
  This option is disabled by default.

  - gw [IP]<HOST-NAME>] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway’s numerical IP address or administrator defined hostname.

- `mint mlcp [ip|ipv6|vlan]`

  **mint**
  Configures MiNT protocol parameters required for MiNT creation and adoption

  **mlcp [ip|ipv6|vlan]**
  Configures the MLCP using the IP address or VLAN. MLCP is used to create a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a wireless controller or service platform, it can be another access point with a path to the wireless controller or service platform.  
  • vlan – Enables MLCP over layer 2 (VLAN) links  
  • ip – Enables MLCP over layer 3 (UDP/IP) links. When enabled, allows adoption over IPv4 address.  
  • ipv6 – Enables MLCP over layer 3 (UDP/IPv6) links. When enabled, allows adoption over IPv6 address.
### mint

- **mint rate-limit level2** [link [ip [<IPv4>|<IPv6>]] [<1-65535>|vlan <1-4094>]] | mlcp [ip|ipv6|vlan] rate <50-1000000> max-burst-size <2-1024> [red-threshold] [background|best-effort|video|voice] <0-100>

**mint**

Configures MiNT protocol parameters required for MiNT creation and adoption

**mint rate-limit level2**

Applies rate limits on extended VLAN traffic.
Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices, or malicious software. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network, and also provides differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server’s response. When such attributes are not present, the settings defined on the controller, service platform or access point are applied. You can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream).

**link [ip <IPv4/IPv6> <1-65535>]|vlan <1-4094>]**

Configures rate limit parameters applicable for all statically configured MiNT links on level2. Select the link-type as ‘IP’ or ‘VLAN’.

- **ip <IPv4/IPv6>** – Configures rate limits for MiNT link traffic over UDP/IP
  - `<IPv4/IPv6>` – Specify the MiNT peer’s IPv4 or IPv6 address in the A.B.C.D and X:X::X:X formats respectively.
  - `<1-65535>` – Configures the virtual port used for rate limiting traffic. Specify the UDP port from 1 - 65535.
- **vlan <1-4094>** – Configures rate limits for MiNT link traffic on specified VLAN
  - `<1-4094>` – Specify the VLAN ID from 1 - 4094.

**mlcp [ip|ipv6|vlan]**

Configures rate limit parameters applicable for MLCP.
MLCP creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be an access point with a path to the controller or service platform.

- **ip** – Configures rate-limits for MLCP over UDP/IP4 links
- **ipv6** – Configures rate-limits for MLCP over UDP/IP6 links
- **vlan** – Configures rate-limits for MLCP over VLAN links

**rate <50-1000000>**

Configures the rate limit from 50 - 1000000 Kbps
This limit constitutes a threshold for the maximum number of packets transmitted or received (from all access categories). Traffic exceeding the defined rate is dropped and a log message is generated. The default setting is 5000 Kbps.

**max-burst-size <2-1024>**

Configures the maximum burst size from 0 - 1024 Kbytes
Smaller the burst size, lesser is the probability of the upstream packet transmission resulting in congestion for the WLAN’s client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 Kbytes.
**red-threshold**

<table>
<thead>
<tr>
<th>traffic type</th>
<th>description</th>
</tr>
</thead>
</table>
| [background]best-effort| Configures the RED threshold for low priority traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%.
| video| Configures the RED threshold for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 25%.
| voice| Configures the RED threshold for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 0%.
| <0-100> | After selecting the traffic type, specify the RED threshold from 0 - 100%.

**mint spf-latency <0-60>**

- Specifies the latency of SPF routing recalculation. This option allows you to set the latency of routing recalculation (within the Shortest Path First (SPF) field). This option is disabled by default.
- <0-60> – Specify the latency from 0 - 60 seconds.

**mint tunnel-across-extended-vlan**

- Enables tunneling of MiNT protocol packets across an extended VLAN. This setting is disabled by default.

**mint tunnel-controller-load-balancing level1**

- Enables load balancing of MiNT extended VLAN traffic across tunnels.
  - level1 – Enables balancing of load of a tunnel wireless controller or service platform over VLAN links.
Examples
rfs7000-37FABE(config-profile-default-rfs7000)#mint level 1 area-id 88
rfs7000-37FABE(config-profile-default-rfs7000)#mint link ip 1.2.3.4 level 2
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
    mint link ip 1.2.3.4 level 2
    mint level 1 area-id 88
    bridge vlan 1
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

| no            | Disables or reverts settings to their default |
7.1.53 misconfiguration-recovery-time

► Profile Config Commands
Verifies connectivity after a configuration is received
Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
misconfiguration-recovery-time [0|<60-300>]

Parameters

• misconfiguration-recovery-time [0|<60-300>]

<table>
<thead>
<tr>
<th>&lt;60-300&gt;</th>
<th>Sets the recovery time from 60 - 300 seconds (default is 180 seconds)</th>
</tr>
</thead>
</table>
| 0         | Disables recovery from misconfiguration

Examples
rfs7000-37FABE(config-profile-default-rfs7000)#misconfiguration-recovery-time 65

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  mint link ip 1.2.3.4
  mint level 1 area-id 88
  bridge vlan 1
  bridging-mode isolated-tunnel
  ...........................................................
  qos trust 802.1p
  interface pppoe1
  use firewall-policy default
  misconfiguration-recovery-time 65
  service pm sys-restart
  router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

| no | Reverts to default (180 seconds) |
7.1.54 **neighbor-inactivity-timeout**

*Profile Config Commands*

Configures neighbor inactivity timeout

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
neighbor-inactivity-timeout <1-1000>
```

**Parameters**

- `neighbor-inactivity-timeout <1-1000>`

| <1-1000> | Sets neighbor inactivity timeout
| --- | ---
| <1-1000> – Specify a value from 1 - 1000 seconds. The default is 30 seconds.

**Examples**

```
rfs7000-37FABE(config-profile-default)#neighbor-inactivity-timeout 500
nrfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000
mint link ip 1.2.3.4
mint level 1 area-id 88
bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
neighbor-inactivity-timeout 500
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote- vpn
crypto ikev2 remote- vpn
crypto auto-ipsec-secure
interface mel
interface gel
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```
### 7.1.55 neighbor-info-interval

**Profile Config Commands**

Configures the neighbor information exchange interval

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

neighbor-info-interval <1-100>

**Parameters**

- neighbor-info-interval <1-100>

| <1-100> | Sets interval from 1 - 100 seconds. The default is 10 seconds. |

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#neighbor-info-interval 6
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  mint link ip 1.2.3.4
  mint level 1 area-id 88
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
neighbor-info-interval 6
neighbor-inactivity-timeout 500
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface me1
interface ge1
  ip dhcp trust
  qos trust dscp
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```
7.1.56 no

Profile Config Commands

Negates a command or resets values to their default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax


Parameters

- no <PARAMETERS>

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

rfs7000-6DCD4B(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface me1
interface ge1
interface ge2
interface ge3
interface ge4
interface pppoe1
use firewall-policy default
service pm sys-restart
adoptor-auto-provisioning-policy-lookup evaluate-always
router ospf
adoption start-delay min 10 max 30
rfs7000-6DCD4B(config-profile-default-rfs7000) #

rfs7000-6DCD4B(config-profile-default-rfs7000)#no adoptor-auto-provisioning-policy-lookup
rfs7000-6DCD4B(config-profile-default-rfs7000)#no adoption start-delay

rfs7000-6DCD4B(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
    interface me1
    interface ge1
    interface ge2
    interface ge3
    interface ge4
    interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
rfs7000-6DCD4B(config-profile-default-rfs7000)#
7.1.57 noc

Profile Config Commands

Configures Network Operations Center (NOC) statistics update interval. This is the interval at which statistical updates are sent by the RF Domain manager to its adopting controller (the NOC controller).

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

coc update-interval [<5-3600>|auto]

Parameters

- noc update-interval [<5-3600>|auto]

| noc update-interval [<5-3600>|auto] | Configures NOC statistics update interval |
|--------------------------------------|------------------------------------------|
|                                       | • <5-3600> – Specify the update interval from 5 - 3600 seconds. |
|                                       | • auto – The NOC statistics update interval is automatically adjusted by the wireless controller or service platform based on load. This option is enabled by default. |

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#noc update-interval 25

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  mint link ip 1.2.3.4
  mint level 1 area-id 88
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  ........................................................
  interface pppoe1
  use firewall-policy default
  misconfiguration-recovery-time 65
  noc update-interval 25
  service pm sys-restart
  router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

| no | Resets NOC related parameters |
7.1.58 ntp

Profile Config Commands

Configures the Network Time Protocol (NTP) server settings

NTP manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Controllers, service platforms, and access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, a controller resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ntp server <PEER-IP/HOSTNAME> {autokey|key|maxpoll|minpoll|prefer|version}
ntp server <PEER-IP/HOSTNAME> {autokey}
ntp server <PEER-IP/HOSTNAME> {maxpoll [1024|2048|4096|8192]}
ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}
ntp server <PEER-IP> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}
ntp server <PEER-IP/HOSTNAME> {prefer version <1-4>|version <1-4> prefer}

Parameters

- ntp server <PEER-IP/HOSTNAME> {autokey} {prefer version <1-4}|version <1-4>

<table>
<thead>
<tr>
<th>ntp server &lt;PEER-IP/HOSTNAME&gt;</th>
<th>Configures NTP server resources that are used to obtain system time</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;PEER-IP/HOSTNAME&gt; — Identifies the NTP server resource by its IP address or hostname. Specify the NTP server’s IP address or hostname.</td>
<td></td>
</tr>
</tbody>
</table>

| autokey | Optional. Enables automatic configuration of authentication key for the specified NTP server. This option is disabled by default. If not enabled, use the 'key' option to configure an authentication key for the NTP server. |

<table>
<thead>
<tr>
<th>ntp server &lt;PEER-IP/HOSTNAME&gt;</th>
<th>Configures NTP server resources that are used to obtain system time</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;PEER-IP/HOSTNAME&gt; — Identifies the NTP server resource by its IP address or hostname. Specify the NTP server’s IP address or hostname.</td>
<td></td>
</tr>
</tbody>
</table>

| maxpoll [1024|2048|4096|8192] | Optional. Configures the maximum polling interval. Once set, the specified NTP server is polled no later than the defined interval. Select one of the following options: |
|--------------------------------|------------------------------------------------------------------|
| • 1024 — Configures the maximum polling interval as 1024 seconds. This is the default setting. |
| • 2048 — Configures the maximum polling interval as 2048 seconds |
| • 4096 — Configures the maximum polling interval as 4096 seconds |
| • 8192 — Configures the maximum polling interval as 8192 seconds |
**ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures NTP server resources that are used to obtain system time</td>
<td>• &lt;PEER-IP/HOSTNAME&gt; – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server’s IP address or hostname.</td>
</tr>
</tbody>
</table>

**minpoll [1024|128|256|512|64]**

Optional. Configures the minimum polling interval. Once set, the specified NTP server is polled no sooner than the defined interval. Select one of the following options:

- 1024 – Configures the minimum polling interval as 1024 seconds
- 128 – Configures the minimum polling interval as 128 seconds
- 256 – Configures the minimum polling interval as 256 seconds
- 512 – Configures the minimum polling interval as 512 seconds
- 64 – Configures the minimum polling interval as 64 seconds. This is the default setting.

**ntp server <PEER-IP/HOSTNAME> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures NTP server resources that are used to obtain system time</td>
<td>• &lt;PEER-IP/HOSTNAME&gt; – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server’s IP address or hostname.</td>
</tr>
</tbody>
</table>

**key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]**

Optional. Defines the authentication key for the specified NTP server. This option is used to configure the key when ‘autokey’ configuration is not enabled.

- <1-65534> – Specify the peer key number. Should not exceed 64 characters in length.
  - md5 – Sets MD5 authentication
  - 0 <WORD> – Configures a clear text password
  - 2 <WORD> – Configures an encrypted password
  - <WORD> – Sets an authentication key

**ntp server <PEER-IP/HOSTNAME> {prefer version <1-4>|version <1-4> prefer}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures NTP server resources that are used to obtain system time</td>
<td>• &lt;PEER-IP/HOSTNAME&gt; – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server’s IP address or hostname.</td>
</tr>
</tbody>
</table>

**prefer version <1-4>**

Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default.

- version – Optional. Configures the NTP version
  - <1-4> – Select the NTP version from 1 - 4. If not specified, the default value of ‘0’ is applied, which implies that the NTP server’s version is ignored.

**version <1-4> prefer**

Optional. Configures the version number used by the specified NTP server resource

- <1-4> – Select the NTP version from 1 - 4. The default setting is 0. A value of ’0’ implies that the NTP server’s version is ignored.
  - prefer – Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default. The NTP version number specified using the ‘version <1-4>’ keyword is applied to this preferred NTP resource.
Examples

rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.10 version 1 prefer

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  mint link ip 1.2.3.4
  mint level 1 area-id 88
  bridge vlan 1
    bridging-mode isolated-tunnel
    ip igmp snooping
    ip igmp snooping querier

interface pppoe1
  use firewall-policy default
  ntp server 172.16.10.10 prefer version 1
  misconfiguration-recovery-time 65
  noc update-interval 25
  service pm sys-restart
  router ospf

rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables or reverts settings to their default</td>
</tr>
</tbody>
</table>
7.1.59 offline-duration

Sets the duration, in minutes, for which a device remains unadopted before it generates offline event.

This command is also supported on the device configuration mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

offline-duration <5-43200>

Parameters

- offline-duration <5-43200>

| offline-duration | Specify a value from 5 - 43200 minutes. The default is 10 minutes. |

Examples

```
rfs4000-229D58(config-profile-test)#offline-duration 200
rfs4000-229D58(config-profile-test)#show context
profile rfs4000 test
  no autoinstall configuration
  no autoinstall firmware
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
    .................................................................
  interface wwan1
  interface pppoe1
  use firewall-policy default
  service pm sys-restart
  router ospf
  offline-duration 200
rfs4000-229D58(config-profile-test)#
```

Related Commands

- no Resets the offline-duration to default (10 minutes)
7.1.60 power-config

Profile Config Commands

Configures the power option mode. Use this command in the profile configuration mode to configure the transmit output power of access point radios. This command is also available in the device-config mode.

Single radio model access points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models. When an access point is powered on for the first time, the system determines the power budget available to the access point. If 802.3af is selected, the access point assumes 12.95 watts is available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts is available.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

power-config [af-option|at-option|mode]

power-config [af-option|at-option] [range|throughput]

power-config mode [auto|3af]

Parameters

- power-config [af-option|at-option] [range|throughput]

<table>
<thead>
<tr>
<th>power-config</th>
<th>Configures the power option mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>af-option</td>
<td>Configures the 802.3.af power mode option. The options are:</td>
</tr>
<tr>
<td>[range</td>
<td>throughput]</td>
</tr>
<tr>
<td></td>
<td>Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates.</td>
</tr>
<tr>
<td></td>
<td>• throughput – Configures the af power throughput mode. This mode provides lower power but has more tx chains. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>Select throughput to transmit packets at the radio’s highest defined basic rate (based on the radio’s current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.</td>
</tr>
</tbody>
</table>
### Examples

```
nx9500-6C8809(config-profile-testAP71XX)#power-config mode 3af

nx9500-6C8809(config-profile-testAP71XX)#power-config af-option range

nx9500-6C8809(config-profile-testAP71XX)#show context
profile ap71xx testAP71XX
  no autoinstall configuration
  no autoinstall firmware
  power-config mode 3af
  power-config af-option range
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
--More--
nx9500-6C8809(config-profile-testAP71XX)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Reverts the power mode setting on this profile to default</td>
</tr>
</tbody>
</table>
7.1.61 preferred-controller-group

Profile Config Commands

Specifies the controller group preferred for adoption

At adoption, an access point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller or service platform for adoption. After selecting the controller or service platform, the access point associates with it and optionally obtains an image upgrade and configuration. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Use this command to specify the controller or service platform preferred for adoption. Once configured, the access point adopts to the specified preferred controller or service platform.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX

Syntax
preferred-controller-group <WORD>

Parameters
- preferred-controller-group <WORD>

Examples
rfs7000-37FABE(config-profile-default-rfs7000)#preferred-controller-group testGroup
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
mint link ip 1.2.3.4
mint level 1 area-id 88
bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  ......................................................
  qos trust 802.1p
interface pppoe1
  use firewall-policy default
  ntp server 172.16.10.10 prefer version 1
  preferred-controller-group testGroup
  misconfiguration-recovery-time 65
  noc update-interval 25
  service pm sys-restart
  router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands
- no Removes the preferred controller group configuration
7.1.62 **preferred-tunnel-controller**

*Profile Config Commands*

Configures the tunnel controller's name preferred for tunneling extended VLAN traffic. Devices using this profile will prefer to route their extended VLAN traffic through the specified tunnel controller (wireless controller or service platform).

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX

**Syntax**

```plaintext
preferred-tunnel-controller <NAME>
```

**Parameters**

- `preferred-tunnel-controller <NAME>`

**Examples**

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000)#preferred-tunnel-controller testtunnel
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the preferred tunnel configuration</td>
</tr>
</tbody>
</table>
### 7.1.63 radius

**Profile Config Commands**

Configures device level RADIUS authentication parameters

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

radius [nas-identifier|nas-port-id] <WORD>

**Parameters**

- `radius [nas-identifier|nas-port-id] <WORD>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius</td>
<td>Configures RADIUS authentication parameters</td>
</tr>
<tr>
<td>nas-identifier &lt;WORD&gt;</td>
<td>Specifies the RADIUS Network Access Server (NAS) identifier attribute used by this device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;WORD&gt;</code> – Specifies the NAS identifier</td>
</tr>
<tr>
<td>nas-port-id &lt;WORD&gt;</td>
<td>Specifies the RADIUS NAS port ID attribute used by this device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;WORD&gt;</code> – Specifies the NAS port ID</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000)#radius nas-port-id 1

rfs7000-37FABE(config-profile-default-rfs7000)#radius nas-identifier test

rfs7000-37FABE(config-profile-default-rfs7000)#show context

profile rfs7000 default-rfs7000
mint link ip 1.2.3.4
mint level 1 area-id 88
bridge vlan 1
    bridging-mode isolated-tunnel
ip igmp snooping
ip igmp snooping querier
radius nas-identifier test
radius nas-port-id 1
neighbor-info-interval 6
neighbor-inactivity-timeout 500
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#

**Related Commands**

- `no` Disables or reverts settings to their default
7.1.64 rf-domain-manager

Profile Config Commands

Configures the RF Domain manager election criteria

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

rf-domain-manager [capable|priority <1-255>]

Parameters

- rf-domain-manager [capable|priority <1-255>]

<table>
<thead>
<tr>
<th>rf-domain-manager</th>
<th>Configures the RF Domain manager election criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>capable</td>
<td>Enables devices using this profile capable of being elected as the RF Domain manager. This option is enabled by default.</td>
</tr>
<tr>
<td>priority &lt;1-255&gt;</td>
<td>Assigns a priority value for devices using this profile in the RF Domain manager election process. The higher the number set, higher is the device’s priority in the RF Domain manager election process.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-255&gt; – Select a priority value from 1 - 255.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#rf-domain-manager priority 9

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  mint link ip 1.2.3.4
  mint level 1 area-id 88

rf-domain-manager priority 9
preferred-controller-group testGroup
misconfiguration-recovery-time 65
noc update-interval 25
service pm sys-restart
preferred-tunnel-controller testtunnel
router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

- no Enables or reverts settings to their default
### 7.1.65 router

#### Profile Config Commands

Enables dynamic routing (BGP and/or OSPF) and enters the routing protocol configuration mode.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

---

**NOTE:** BGP is supported only on RFS4000, RFS6000, NX4500, NX6500, NX75XX, NX9000 and NX9500 model controllers and service platforms.

The access points only support OSPF routing.

The NX9500 and NX9510 service platforms do not support OSPF routing.

---

**Syntax**

```
router [bgp|ospf]
```

**Parameters**

- `router [bgp|ospf]`

<table>
<thead>
<tr>
<th>router</th>
<th>Enables dynamic routing and enters the routing protocol configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Enables BGP dynamic routing and configures relevant settings. BGP is an inter-ISP routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between Autonomous Systems (AS) on the Internet. BGP uses TCP as its transport protocol, eliminating the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. Routing information exchanged through BGP supports destination based forwarding only. It assumes a router forwards packets based on the destination address carried in the IP header of the packet. An AS is a set of routers under the same administration that use Interior Gateway Protocol (IGP) and common metrics to define how to route packets within the AS. For more information on dynamic BGP routing configurations, see BORDER GATEWAY PROTOCOL.</td>
</tr>
<tr>
<td>ospf</td>
<td>Enables OSPF dynamic routing and configures relevant settings. Changes configuration mode to router mode. OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. For more information on dynamic OSPF routing configurations, see ROUTER-MODE COMMANDS.</td>
</tr>
</tbody>
</table>
Examples

```
rfs7000-37FABE(config-profile-default-rfs7000)#router ospf
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#?
```

Router OSPF Mode commands:
- `area` OSPF area
- `auto-cost` OSPF auto-cost
- `default-information` Distribution of default information
- `ip` Internet Protocol (IP)
- `network` OSPF network
- `no` Negate a command or set its defaults
- `ospf` Ospf
- `passive` Make OSPF Interface as passive
- `redistribute` Route types redistributed by OSPF
- `route-limit` Limit for number of routes handled OSPF process
- `router-id` Router ID
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables OSPF settings</td>
</tr>
</tbody>
</table>
7.1.66 spanning-tree

Profile Config Commands
Enables spanning tree commands. Use these commands to configure the errdisable, multiple spanning tree and portfast settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
spanning-tree [errdisable|mst|portfast]
spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]
spanning-tree mst [<0-15>|cisco-interoperability|enable|forward-time|hello-time|
  instance|max-age|max-hops|region|revision]
spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability [enable|disable]|
  enable|forward-time <4-30>|hello-time <1-10>|instance <1-15>|max-age <6-40>|
  max-hops <7-127>|region <LINE>|revision <0-255>]
spanning-tree portfast [bpdufilter|bpduguard] default

Parameters
- spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]

<table>
<thead>
<tr>
<th>spanning-tree</th>
<th>Configures spanning-tree related parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>errdisable</td>
<td>Disables or shutdown ports where traffic is looping, or ports with traffic in one direction</td>
</tr>
<tr>
<td>recovery</td>
<td>Enables the timeout mechanism for a port to be recovered. This option is disabled by default.</td>
</tr>
</tbody>
</table>
| cause bpduguard | Specifies the reason for errdisable  
  • bpduguard – Recovers from errdisable due to bpduguard |
| interval <10-1000000> | Specifies the interval after which a port is enabled  
  • <10-1000000> – Specify a value from 10 - 1000000 seconds. The default is 300 seconds. |

- spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability [enable|disable]|
  enable|forward-time <4-30>|hello-time <1-10>|instance <1-15>|max-age <6-40>|
  max-hops <7-127>|region <LINE>|revision <0-255>]

<table>
<thead>
<tr>
<th>spanning-tree</th>
<th>Configures Multiple Spanning Tree (MST) commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>mst</td>
<td>The MSTP provides an extension to STP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.</td>
</tr>
</tbody>
</table>
### spanning-tree.portfast [bpdufilter|bpduguard] default

**spanning-tree**

Configures spanning-tree related parameters.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| portfast [bpdufilter| bpduguard] default | Enables PortFast on a bridge  
  - bpdufilter default – Sets the BPDU filter for the port. The BPDU filter is disabled by default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures that PortFast enabled ports do not transmit or receive BPDUs.  
  - bpduguard default – Guards PortFast ports against BPDU receive. The BPDU guard is disabled by default. Enabling the BPDU guard means this port will shutdown on receiving a BPDU.  
  - default – Enables the BPDU filter and/or BPDU guard on PortFast enabled ports by default. |

### Other Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| <0-15> priority <0-61440> | Specifies the number of instances required to configure MST. Select a value from 0 -15.  
  - priority – Sets the bridge priority to the specified value. This value is used to determine the root bridge. Use the no parameter with this command to restore the default bridge priority value.  
  - <0-61440> – Sets the bridge priority in increments (Lower priority indicates greater likelihood of becoming root). |
| cisco interoperability [enable|disable] | Enables CISCO interoperability  
  Enables interoperability with CISCO's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default. |
| enable | Enables MST protocol |
| forward-time <4-30> | Specifies the forwarding delay time in seconds  
  - <4-30> – Specify a value from 4 - 30 seconds. The default is 15 seconds. |
| hello-time <1-10> | Specifies the hello BDPU interval in seconds  
  - <1-10> – Specify a value from 1 - 10 seconds. The default is 2 seconds. |
| instance <1-15> | Defines the instance ID to which the VLAN is associated  
  - <1-15> – Specify an instance ID from 1 - 10. |
| max-age <6-40> | Defines the maximum time to listen for the root bridge  
  - <6-40> – Specify a value from 4 - 60 seconds. The default is 20 seconds. |
| max-hops <7-127> | Defines the maximum hops when BPDU is valid  
  - <7-127> – Specify a value from 7 - 127. The default is 20. |
| region <LINE> | Specifies the MST region  
  - <LINE> – Specify the region name. |
| revision <0-255> | Sets the MST bridge revision number. This enables the retrieval of configuration information.  
  - <0-255> – Specify a value from 0 - 255. This default is 0. |
Usage Guidelines

If a bridge does not hear BPDUs from the root bridge within the specified interval, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

MSTP is based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Wireless Controllers or service platforms with the same instance, VLAN mapping, revision number and region names define a unique region. Wireless Controllers or service platforms in the same region exchange BPDUs with instance record information within.

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#spanning-tree errdisable recovery cause bpduguard

rfs7000-37FABE(config-profile-default-rfs7000)#spanning-tree mst 2 priority 4096

rfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000
mint link ip 1.2.3.4
mint level 1 area-id 88
bridge vlan 1
   bridging-mode isolated-tunnel
   ip igmp snooping
   ip igmp snooping querier
   radius nas-identifier test
   radius nas-port-id 1
neighbor-info-interval 6
neighbor-inactivity-timeout 500
spanning-tree mst 2 priority 4096
spanning-tree errdisable recovery cause bpduguard
autoinstall configuration
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables or reverts settings to their default</td>
</tr>
</tbody>
</table>
### 7.1.67 traffic-class-mapping

#### Profile Config Commands

Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority. This mapping is required to provide priority of service to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic. Devices use the traffic class field in the IPv6 header to set this priority. This command allows you to assign a priority for different IPv6 traffic types.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>
```

#### Parameters
- **traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>**

<table>
<thead>
<tr>
<th>traffic-class-mapping</th>
<th>Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPv6-TRAFFIC-CLASS-VALUE&gt;</td>
<td>Specify the traffic class value of incoming IPv6 untagged packet(s) (could be a single value or a list. For example, 10-20, 25, 30-35). This is the DSCP 6-bit parameter in the header of every IP packet used for packet classification.</td>
</tr>
<tr>
<td>priority &lt;0-7&gt;</td>
<td>Specify the 802.1p priority to map with the traffic-class value specified in the previous step</td>
</tr>
<tr>
<td>· &lt;0-7&gt;</td>
<td>Specify a value from 0 - 7.</td>
</tr>
</tbody>
</table>

**Note:** The 802.1p priority is a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:
- 0 – Best Effort
- 1 – Background
- 2 – Spare
- 3 – Excellent Effort
- 4 – Controlled Load
- 5 – Video
- 6 – Voice
- 7 – Network Control
Examples

rfs4000-229D58 (config-profile-TestRFS4000)#traffic-class-mapping 25 priority 2

rfs4000-229D58 (config-profile-TestRFS4000)#show context
profile rfs4000 TestRFS4000
  traffic-class-mapping 25 priority 2
  no autoinstall configuration
  no autoinstall firmware
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
  crypto remote-vpn-client

-More-
rfs4000-229D58 (config-profile-TestRFS4000)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes mapping between IPv6 traffic class value (of incoming IPv6 untagged packets) and 802.1p priority</td>
</tr>
</tbody>
</table>
7.1.68 traffic-shape

Profile Config Commands

Enables traffic shaping and configures traffic shaping parameters. This command is applicable to both the profile and device configuration modes.

Traffic shaping is a means of regulating data transfers and ensuring a specific level of performance within a network. Traffic shaping does the following:

- Controls flow of packets based on their priority value. Prioritized traffic streams are given priority over less important traffic.
- Controls traffic on an interface to match its flow to the speed of a remote target’s interface and ensure traffic conforms to applied policies
- Shapes traffic to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Use this option to apply traffic shaping to specific applications or application categories. Note, in scenarios where a traffic class is matched against an application, application-category, and ACL rule, the application rule will be applied first, followed by the application-category, and finally the ACL. Further, using traffic shaping, an application takes precedence over an application category.

To enable traffic shaping, configure QoS values on the basis of which priority of service is provided to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic. For configuring IPv6 traffic class mappings, see traffic-class-mapping. And for configuring DSCP traffic class mappings, see dscp-mapping.

Supported in the following platforms:

- Access Points — AP622, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530

Syntax

```
traffic-shape [activation-criteria|app-category|application|class|enable|priority-map|total-bandwidth]

traffic-shape activation-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]

traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>

traffic-shape application <APPLICATION-NAME> class <1-4>

traffic-shape class <1-4> [max-buffers|max-latency|rate]

traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>|red-percent <1-100>}

traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]

traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]|total-bandwidth-percent <1-100>]
```

**NOTE:** The available range for the ‘rate’ field will vary depending on the unit selected. It is 250 - 250000 for Kbps and 1 - 250 for Mbps.

```
traffic-shape priority-map <0-7>

traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]
```
NOTE: The available range for the 'total-bandwidth' field will vary depending on the unit selected. It is 250 - 1000000 for Kbps and 1 - 1000 for Mbps.

traffic-shape enable

Parameters

- **traffic-shape activation-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]**

<table>
<thead>
<tr>
<th>traffic-shape activation-criteria</th>
<th>Configures traffic-shape activation criteria that determines when the device invokes traffic shaping</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>Always invokes traffic shaping. This is the default setting.</td>
</tr>
<tr>
<td>cluster-master</td>
<td>Invokes traffic shaping when the device is the cluster master. The solitary cluster master (elected using a priority assignment scheme) is a cluster member that provides management configuration and Smart RF data to other members within the cluster. Cluster requests go through the elected master before dissemination to other cluster members.</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Invokes traffic shaping when the device is the RF Domain manager. The RF Domain manager is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain.</td>
</tr>
<tr>
<td>vrrp-master &lt;1-255&gt;</td>
<td>Invokes traffic shaping when the device is the VRRP master. As the VRRP master, the device responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-255&gt; – Specify the VRRP group ID from 1 - 255.</td>
</tr>
</tbody>
</table>

- **traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>**

<table>
<thead>
<tr>
<th>traffic-shape app-category &lt;APP-CATEGORY-NAME&gt; class &lt;1-4&gt;</th>
<th>Configures an application category to traffic-class mapping. Use this option to apply an application category to traffic-shaper class mapping. Naming and categorizing applications that do not fall into existing groups is an additional means of filtering and potentially limiting network airtime to consumptive non required applications negatively impacting network performance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• app-category &lt;APP-CATEGORY-NAME&gt; – Specify the application category name. To list the available application categories, press [TAB] after entering app-category. Select the required category from the displayed list.</td>
</tr>
<tr>
<td></td>
<td>• class &lt;1-4&gt; – Map the specified application category to a traffic-shaper class from 1 - 4.</td>
</tr>
</tbody>
</table>

**Note:** Before configuring an application category to class mapping, ensure that the specified classes have been configured. Use the 'class > [max-buffers|max-latency|rate]' option available with this command to configure a traffic shaper class. For more information, see following parameter tables.
### Traffic-Shape Application Configuration

- **traffic-shape application <APPLICATION-NAME> class <1-4>**

  Configures an application to traffic-class mapping. Use this option to apply an application to traffic-shaper class mapping.
  - app-category <APPLICATION-NAME> – Specify the application name.
  - class <1-4> – Map the specified application to a traffic-shaper class from 1 - 4.

  **Note:** Before configuring an application to class mapping, ensure that the specified classes have been configured. Use the `class > [max-buffers|max-latency|rate]` option available with this command to configure a traffic shaper class. For more information, see following tables.

### Traffic-Shape Class Configuration

- **traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>|red-percent <1-100>}

  Configures the queue length limit for different traffic-shaper class
  - class <1-4> – Specify the traffic-shaper class from 1 - 4.
  - max-buffers <1-400> – Configures the maximum queue length for packets of different priority queues, after which the queue starts to drop packets.
    - <1-400> – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.

  **Note:** For access points the upper queue length limit is 400.

- **red-level <1-400>**

  Optional. Performs *Random Early Drop* (RED) when a specified queue length in packets is reached
  - <1-400> – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.

  The RED algorithm is a queueing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped.

  **Note:** For more information on default values, see the Usage Guidelines section in this topic.

- **red-percent <1-100>**

  Optional. Performs RED when a specified value, which is a percentage of the max-buffers configured, is reached
  - <1-100> – Configure the percentage of the max-buffers from 1 - 100 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.

### Max-Latency Configuration

- **traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]**

  Configures the max-latency for different traffic-shaper class. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8.
  - class <1-4> – Specify the traffic-shaper class from 1 - 4.
  - max-latency <1-1000000> – Configures the max-latency for packets of different priority queues, after which the queue starts to drop packets.
    - <1-1000000> – Configure the max-latency from 1 - 100000 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.
    - [msec|usec] – Configures the unit for measuring latency as milliseconds (msec) or microseconds (usec). The default setting is msec.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]|total-bandwidth-percent <1-100> | Configures traffic rate, in either Kbps, Mbps or percentage, for the different traffic shaper class. Specify rates for different traffic shaper class to control the maximum traffic rate sent or received on an interface. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.  
  - class <1-4> – Specify the traffic-shaper class from 1 - 4.  
  - <1-250000> – Specify the rate from 1 - 250000.  
  - [Kbps|Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Kbps.  
  **Note:** The range varies depending on the unit selected. It is 1 - 250 Mbps, or 250 - 250000 Kbps.  
  - total-bandwidth-percent <1-100> – Specify the traffic rate from 1 - 100% of the total bandwidth. |
| traffic-shape priority-map <0-7>             | Configures the traffic-shaper queues, within a class, having different priority values (0, 1, 2, 3, 4, 5, 6, and 7). There are 8 queues (0 - 7), and traffic is queued in each based on the incoming packet’s 802.1p 3-bit priority markings.  
  - priority-map <0-7> – Specify the priority from 0 - 7 for priority levels 0, 1, 2, 3, 4, 5, 6, and 7.  
  The IEEE 802.1p standards sets a 3-bit value in the MAC header to indicate prioritization. This 3-bit value provides priority levels ranging from 0 to 7 (i.e., a total of 8 levels), with level 7 representing the highest priority. This permits packets to cluster and form different traffic classes. In case of network congestion, packets with higher priority receive preferential treatment while low priority packets are kept on hold. |
| traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps] | Configures the total-bandwidth for traffic shaping  
  - <1-1000000> – Specify the value from 1 - 1000000 Kbps/Mbps. The default value is 10 Mbps.  
  - [Kbps|Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Mbps.  
  **Note:** The range varies depending on the unit selected. It is 1 - 1000 Mbps, or 250 - 1000000 Kbps. |
| traffic-shape enable                         | Enables traffic shaping using the defined bandwidth, rate and class mappings configured using this command  
  **Note:** Traffic shaping is disabled by default. |
### Usage Guidelines

Following are the default max-buffers set for the traffic shaper classes:

```
traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
```

Following is the default priority-map settings:

```
traffic-shape priority-map 2 0 1 3 4 5 6 7
```

### Examples

```bash
nx9500-6C8809(config-profile-ProfileNX5500)#show context include-factory | include traffic-shape
traffic-shape priority-map 2 0 1 3 4 5 6 7
traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape activation-criteria always
traffic-shape total-bandwidth 10 Mbps
no traffic-shape enable
```

```bash
nx9500-6C8809(config-profile-ProfileNX5500)##traffic-shape enable
```

```bash
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape class 1 rate 250 Mbps
```

```bash
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape application Bing class 1
```

```bash
nx9500-6C8809(config-profile-ProfileNX5500)#show context include-factory | include traffic-shape
traffic-shape priority-map 2 0 1 3 4 5 6 7
traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape activation-criteria always
traffic-shape application Bing class 1
traffic-shape total-bandwidth 200 Mbps
traffic-shape enable
```

nx9500-6C8809(config-profile-ProfileNX5500)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes traffic shaping configuration or reverts them to the default values</td>
</tr>
</tbody>
</table>
**7.1.69 trustpoint (profile-config-mode)**

*Profile Config Commands*

Configures the trustpoint assigned for validating a CMP auth Operator.

A certificate links identity information with a public key enclosed in the certificate.

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain the CA certificate in its Trusted Root Library so it can trust certificates signed by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

---

**NOTE:** Certificates/trustpoints used in this command should be verifiable as existing on the device.

---

**NOTE:** For information on configuring trustpoints on a device, see `trustpoint (device-config-mode)`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
trustpoint [cmp-auth-operator|radius-ca|radius-server] <TRUSTPOINT-NAME>
```

**Parameters**

- `trustpoint [cmp-auth-operator|radius-ca|radius-server] <TRUSTPOINT-NAME>`

<table>
<thead>
<tr>
<th>trustpoint</th>
<th>Assigns an existing trustpoint to validate CMP auth operator, client certificates, and RADIUS server certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmp-auth-operator</td>
<td>Assigns an existing trustpoint to validate CMP auth operator Once validated, CMP is used to obtain and manage digital certificates in a PKI network. Digital certificates link identity information with a public key enclosed within the certificate, and are issued by the CA. Use this command to specify the CMP-assigned trustpoint. When specified, devices send a certificate request to the CMP supported CA server, and download the certificate directly from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.</td>
</tr>
<tr>
<td>radius-ca</td>
<td>Assigns an existing trustpoint to validate client certificates in EAP</td>
</tr>
</tbody>
</table>
Examples

nx9500-6C8809(config-profile-testNX9000)#trustpoint cmp-auth-operator test

nx9500-6C8809(config-profile-testNX9000)#show context
profile nx9000 testNX9000
  no autoinstall configuration
  no autoinstall firmware
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  ..............................................................
  service pm sys-restart
  router bgp
  trustpoint cmp-auth-operator test
nx9500-6C8809(config-profile-testNX9000)#
### 7.1.70 tunnel-controller

*Profile Config Commands*

Configures the tunneled WLAN (extended VLAN) wireless controller or service platform’s name

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

tunnel-controller <NAME>

**Parameters**

- tunnel-controller <NAME>

<table>
<thead>
<tr>
<th>tunnel-controller &lt;NAME&gt;</th>
<th>Configures the tunneled WLAN (extended VLAN) wireless controller or service platform’s name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>•  &lt;NAME&gt; – Specify the name.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-profile-default-rfs7000)#tunnel-controller testgroup

**Related Commands**

- **no**

  Removes the configured the tunneled WLAN (extended VLAN) wireless controller or service platform’s name
7.1.71 use

Profile Config Commands

Associates existing policies with this profile. This command is also applicable to the device configuration mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax Profiles Mode


Syntax Device Mode


NOTE: The following tables contain the ‘use’ command parameters for the Profile and Device configuration modes.

<table>
<thead>
<tr>
<th>Parameters Profiles Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associates the specified policies with this profile</td>
</tr>
<tr>
<td>The specified policies should be existing and configured.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>auto-provisioning-policy &lt;POLICY-NAME&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associates an auto provisioning policy</td>
</tr>
<tr>
<td>The specified policies should be existing and configured.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bonjour-gw-forwarding-policy &lt;POLICY-NAME&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses an existing Bonjour GW Forwarding policy with a profile or device</td>
</tr>
<tr>
<td>&lt;POLICY-NAME&gt; – Specify the Bonjour GW Forwarding policy name (should be existing and configured).</td>
</tr>
</tbody>
</table>

**Note:** For more information on Bonjour GW Forwarding policy, see [bonjour-gw-forwarding-policy](#).

<table>
<thead>
<tr>
<th>bonjour-gw-query-forwarding-policy &lt;POLICY-NAME&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses an existing Bonjour GW Query Forwarding policy with a profile or device</td>
</tr>
<tr>
<td>&lt;POLICY-NAME&gt; – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).</td>
</tr>
<tr>
<td>Command Name</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
</tbody>
</table>
| captive-portal server        | Configures access to a specified captive portal with this profile  
| <CAPTIVE-PORTAL>             | • <CAPTIVE-PORTAL> – Specify the captive portal name.                                                                                                                                                                                                                         |
| client-identity-identity-group | Associates an existing client identity group with this profile  
| <CLIENT-IDENTITY-GROUP-NAME> | • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name.  
| Note: For more information on the ‘client-identity’ and ‘client-identity-group’ commands, see client-identity and client-identity-group.                                                                 |                                                                                                                                                                                                             |
| crypto-cmp-policy            | Associates an existing crypto certificate management protocol (CMP) policy with this profile  
| <POLICY-NAME>                | • <POLICY-NAME> – Specify the CMP policy name.  
| For more information on configuring a crypto CMP policy, see CRYPTO-CMP-POLICY.                          |                                                                                                                                                                                                             |
| dhcp-server-policy           | Associates a DHCP server policy  
| <DHCP-POLICY>                | • <DHCP-POLICY> – Specify the DHCP server policy name.                                                                                                                                                                                                                         |
| dhcpv6-server-policy         | Associates a DHCPv6 server policy  
| <DHCPv6-POLICY>              | • <DHCPv6-POLICY> – Specify the DHCPv6 server policy name.                                                                                                                                                                                                                      |
| event-system-policy          | Associates an event system policy  
| <EVENT-SYSTEM-POLICY>        | • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.                                                                                                                                                                                                                  |
| firewall-policy              | Associates a firewall policy  
| <FW-POLICY>                  | • <FW-POLICY> – Specify the firewall policy name.                                                                                                                                                                                                                             |
| global-assoc-list server     | Associates the specified global association list with the controller profile  
| <GLOBAL-ASSOC-LIST-NAME>     | • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name.  
| Once associated, the controller, using this profile, applies this association list to requests received from all adopted APs. For more information on global association list, see global-association-list. |                                                                                                                                                                                                             |
| guest-management             | Associates the specified guest management policy with the controller profile  
| <GUEST-MANAGEMENT-POLICY-NAME> | • <GUEST-MANAGEMENT-POLICY-NAME> – Specify the guest management policy name (should be existing and configured).                                                                                     |
| management-policy            | Associates a management policy  
| <MNGT-POLICY>                | • <MNGT-POLICY> – Specify the management policy name.                                                                                                                                                                                                 |                                                                                                                                                                                                             |
| radius-server-policy         | Associates a device onboard RADIUS policy  
| <RADIUS-POLICY>              | • <RADIUS-POLICY> – Specify the RADIUS policy name.                                                                                                                                                                                                                          |
| role-policy                  | Associates a role policy  
| <ROLE-POLICY>                | • <ROLE-POLICY> – Specify the role policy name.                                                                                                                                                                                                                           |
| routing-policy               | Associates a routing policy  
| <ROUTING-POLICY>             | • <ROUTING-POLICY> – Specify the routing policy name.  
| This is not applicable to the NX45XX and NX65XX series profiles.                                         |                                                                                                                                                                                                             |
| smart-cache-policy           | Associates an existing Smart Cache policy with a profile or device  
| <POLICY-NAME>                | • <POLICY-NAME> – Specify the policy name.                                                                                                                                                                                                                                 |
| web-filter-policy            | Associates an existing Web Filter policy with a profile or device  
| <POLICY-NAME>                | • <POLICY-NAME> – Specify the policy name.                                                                                                                                                                                                                                 |
## Parameters Device Mode


<table>
<thead>
<tr>
<th>use</th>
<th>Associates the following policies with this device:</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-provisioning-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Associates an auto provisioning policy</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;POLICY-NAME&gt;</code> – Specify the auto provisioning policy name.</td>
</tr>
<tr>
<td>bonjour-gw-forwarding-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Uses an existing Bonjour GW Forwarding policy with a profile or device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;POLICY-NAME&gt;</code> – Specify the Bonjour GW Forwarding policy name (should be existing and configured).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For more information on Bonjour GW Forwarding policy, see <code>bonjour-gw-forwarding-policy</code>.</td>
</tr>
<tr>
<td>bonjour-gw-query-forwarding-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Uses an existing Bonjour GW Query Forwarding policy with a profile or device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;POLICY-NAME&gt;</code> – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).</td>
</tr>
<tr>
<td>captive-portal server <code>&lt;CAPTIVE-PORTAL&gt;</code></td>
<td>Configures access to a specified captive portal</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;CAPTIVE-PORTAL&gt;</code> – Specify the captive portal name.</td>
</tr>
<tr>
<td>client-identity-group <code>&lt;CLIENT-IDENTITY-GROUP-NAME&gt;</code></td>
<td>Associates an existing client identity group with this device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;CLIENT-IDENTITY-GROUP-NAME&gt;</code> – Specify the client identity group name.</td>
</tr>
<tr>
<td></td>
<td>For more information on the 'client-identity' and 'client-identity-group' commands, see <code>client-identity</code> and <code>client-identity-group</code>.</td>
</tr>
<tr>
<td>crypto-cmp-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Associates an existing crypto certificate management protocol (CMP) policy with this profile</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;POLICY-NAME&gt;</code> – Specify the CMP policy name.</td>
</tr>
<tr>
<td></td>
<td>For more information on configuring a crypto CMP policy, see <code>CRYPTO-CMP-POLICY</code>.</td>
</tr>
<tr>
<td>dhcp-server-policy <code>&lt;DHCP-POLICY&gt;</code></td>
<td>Associates a DHCP server policy</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DHCP-POLICY&gt;</code> – Specify the DHCP server policy name.</td>
</tr>
<tr>
<td>dhcpv6-server-policy <code>&lt;DHCPv6-POLICY&gt;</code></td>
<td>Associates a DHCPv6 server policy</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DHCPv6-POLICY&gt;</code> – Specify the DHCPv6 server policy name.</td>
</tr>
<tr>
<td>event-system-policy <code>&lt;EVENT-SYSTEM-POLICY&gt;</code></td>
<td>Associates an event system policy</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;EVENT-SYSTEM-POLICY&gt;</code> – Specify the event system policy name.</td>
</tr>
<tr>
<td>firewall-policy <code>&lt;FW-POLICY&gt;</code></td>
<td>Associates a firewall policy</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;FW-POLICY&gt;</code> – Specify the firewall policy name.</td>
</tr>
<tr>
<td>global-association-list server <code>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</code></td>
<td>Associates the specified global association list with the device (controller)</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</code> – Specify the global association list name.</td>
</tr>
<tr>
<td></td>
<td>Once associated, the controller applies this association list to requests received from all adopted APs. For more information on global association list, see <code>global-association-list</code>.</td>
</tr>
</tbody>
</table>
### Examples

```
rfs7000-37FABE(config-profile-default-rfs7000)#use event-system-policy
TestEventSysPolicy

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  mint link ip 1.2.3.4
  mint level 1 area-id 88
  ....................................................
  interface ge3
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
  interface ge4
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
  interface pppoe1
  use event-system-policy TestEventSysPolicy
```
use firewall-policy default
ntp server 172.16.10.10 prefer version 1
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disassociates a specified policy from this profile</td>
</tr>
</tbody>
</table>
7.1.72 **vrrp**

*Profile Config Commands*

Configures VRRP group settings

A default gateway is a critical resource for connectivity. However, it is prone to a single point of failure. Thus, redundancy for the default gateway is required. If WAN backhaul is available, and a router failure occurs, then the controller should act as a router and forward traffic on to its WAN link.

Define an external VRRP configuration when router redundancy is required in a network requiring high availability.

Central to VRRP configuration is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router’s MAC address
- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.

The nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
vrrp [<1-255>|version]

vrrp <1-255> [delta-priority|description|interface|ip|monitor|preempt|priority|
  sync-group|timers]

vrrp <1-255> [delta-priority <1-253>|description <LINE>|ip <IP> {<IP>}
  |preempt {delay <1-65535>}}|priority <1-254>|sync-group]

vrrp <1-255> interface vlan <1-4094>

vrrp <1-255> monitor [{<IF-NAME>|critical-resource|pppoe1|vlan|wwan1}] 
  vrrp <1-255> monitor [{<IF-NAME}|pppoe1|vlan <1-4094>|wwan1} {<IF-NAME>|
  critical-resource|pppoe1|vlan|wwan1}]

vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3> <CRM-NAME4> 
  {action [decrement-priority|increment-priority] {<IF-NAME>|pppoe1|vlan|wwan1}}

vrrp <1-255> timers advertise [<1-255]|centiseconds <25-4095>|msec <250-999>]

vrrp version [2|3]
```
### Parameters

- **vrrp <1-255>** [delta-priority <1-253>|description <LINE>|vrrp ip <IP> {<IP>|preempt {delay <1-65535>}}|priority <1-254}|sync-group]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp &lt;1-255&gt;</td>
<td>Configures the virtual router ID from 1-255. Identifies the virtual router the packet is reporting status for.</td>
</tr>
</tbody>
</table>
| delta-priority <1-253> | Configures the priority to decrement (local link monitoring and critical resource monitoring) or increment (critical resource monitoring). When the monitored interface is down, the configured priority decrements by a value defined by the delta-priority option. When monitoring critical resources, the value increments by the delta-priority option.  
  - <1-253> – Specify the delta priority level from 1-253. |
| description <LINE> | Configures a text description for the virtual router to further distinguish it from other routers with similar configuration  
  - <LINE> – Provide a description (a string from 1-64 characters in length) |
| ip <IP-ADDRESSES> | Identifies the IP address(es) backed by the virtual router. These are IP addresses of Ethernet switches, routers, and security appliances defined as virtual router resources.  
  - <IP-ADDRESSES> – Specify the IP address(es) in the A.B.C.D format. This configuration triggers VRRP operation. |
| preempt {delay <1-65535>} | Controls whether a high priority backup router preempts a lower priority master. This field determines if a node with higher priority can takeover all virtual IPs from a node with lower priority. This feature is disabled by default.  
  - delay – Optional. Configures the pre-emption delay timer from 1 - 65535 seconds (default is 0 seconds). This option can be used to delay sending out the master advertisement or, in case of monitored link coming up, adjusting the VRRP priority by priority delta. |
| priority <1-254> | Configures the priority level of the router within a VRRP group. This value determines which node is elected as the Master. Higher values imply higher priority, value 254 has the highest precedence (default is 100). |
| sync-group | Adds this VRRP group to a synchronized group. To trigger VRRP failover, it is essential all individual groups within a synchronized group have failover. VRRP failover is triggered if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This feature is disabled by default. |

- **vrrp <1-255> interface vlan <1-4094>**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp &lt;1-255&gt;</td>
<td>Configures the virtual router ID from 1-255. Identifies the virtual router the packet is reporting status for.</td>
</tr>
</tbody>
</table>
| interface     | Enables VRRP on the specified switch VLAN interface (SVI)  
  - vlan <1-4094> – Specify the VLAN interface ID from 1 - 4094. |

- **vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3> <CRM-NAME4> {action [decrement-priority|increment-priority] {<IF-NAME>|pppe1|vlan|wwan1}}**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp &lt;1-255&gt;</td>
<td>Configures the virtual router ID from 1-255. Identifies the virtual router the packet is reporting status for.</td>
</tr>
<tr>
<td>monitor</td>
<td>Enables link monitoring or <em>Critical Resource Monitoring</em> (CRM)</td>
</tr>
</tbody>
</table>
### vrrp version [2|3]

Sets the action on critical resource down event. It is a recursive parameter that sets the action for each of the four critical resources being monitored.

- **decrement-priority** – Decrements the priority of virtual router on critical resource down event
- **increment-priority** – Increments the priority of virtual router on critical resource down event

### action [decrement-priority|increment-priority]

Optional. Enables interface monitoring

- **<IF-NAME>** – Specify the interface name to monitor

### vlan <1-4094>

Optional. Enables VLAN (switched virtual interface) interface monitoring

- **<1-4094>** – Specify the VLAN interface ID from 1-4094.

### critical-resource <CRM-NAME1>

Specifies the name of the critical resource to monitor. VRRP can be configured to monitor maximum of four critical resources. Use the `<CRM-NAME2>`, `<CRM-NAME3>`, and `<CRM-NAME4>` to provide names of the remaining three critical resources.

By default VRRP is configured to monitor all critical resources on the device.

### timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]

Configures the VRRP advertisements time interval. This is the interval at which a master sends out advertisements on each of its configured VLANs.

- **<1-255>** – Configures the timer interval from 1-255 seconds. (applicable for VRRP version 2 only)
- **centiseconds <25-4095>** – Configures the timer interval in centiseconds (1/100th of a second). Specify a value between 25 - 4095 centiseconds (applicable for VRRP version 3 only).
- **msec <250-999>** – Configures the timer interval in milliseconds (1/1000th of a second). Specify a value between 250 - 999 msec (applicable for VRRP version 2 only).

Default is 1 second.

### Examples

```conf
rfs7000-37FABE(config-profile-default-rfs7000)#vrrp version 3
rfs7000-37FABE(config-profile-default-rfs7000)#vrrp 1 sync-group
rfs7000-37FABE(config-profile-default-rfs7000)#vrrp 1 delta-priority 100
```
```plaintext
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  ......................................................
  vrrp 1 timers advertise 1
  vrrp 1 preempt
  vrrp 1 sync-group
  vrrp 1 delta-priority 100
  vrrp version 3
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Reverts VRRP settings</td>
</tr>
</tbody>
</table>

### 7.1.73 vrrp-state-check

#### Profile Config Commands

Publishes interface via OSPF or BGP based on **Virtual Router Redundancy Protocol (VRRP)** status

VRRP allows automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This option is enabled by default.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

#### Syntax

```
vrrp-state-check
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#vrrp-state-check
```
```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
```
```
nx9000 B4-C7-99-6C-88-09
    use profile default-nx9000
    use rf-domain default
    no weight
    no timers bgp
    ip default-gateway priority 7500
    bgp-route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 360
    **vrrp-state-check**
    controller adopted-devices controllers
    alias string $SN B4C7996C8809
```
```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables the publishing of an interface via OSPF/BGP based on VRRP status</td>
</tr>
</tbody>
</table>
### 7.1.74 **wep-shared-key-auth**

#### Profile Config Commands

Enables support for 802.11 WEP shared key authentication

When enabled, devices, using this profile, use a WEP key to access the network. The controller or service platform use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without the recommended adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`wep-shared-key-auth`

**Parameters**

None

**Examples**

```bash
rfs7000-37FABE(config-profile-default-rfs7000)#wep-shared-key-auth
rfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000
bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
  **wep-shared-key-auth**
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface mel
  interface gel
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
    interface ge2
      ip dhcp trust
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disable support for 802.11 WEP shared key authentification</td>
</tr>
</tbody>
</table>
**7.1.75 service**

> **Profile Config Commands**

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
service [cluster|critical-resource|fast-switching|enable|global-association-list|
lldp|memory|meshpoint|pm|power-config|radius|remote-config|rss-timeout|watchdog|
wireless|show]
```

```
service cluster master-election immediate

service critical-resource port-mode-source-ip <IP>

service enable [l2tpv3|pppoe|radiusd]

service global-association-list blacklist-interval <1-65535>

service lldp loop-detection

service memory kernel decrease

service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-5>|port-channel <1-2>|up1]

service pm sys-restart

service power-config [3af-out|force-3at]

service radius dynamic-authorization additional-port <1-65535>

service remote-config apply-delay <0-600>

service rss-timeout <0-86400>

service watchdog

service wireless [anqp-frag-always|anqp-frag-size|ap650|client|cred-cache-sync|
inter-ap-key|noise-immunity|reconfig-on-tx-stall|test|wispe-controller-port]

service wireless anqp-frag-always

service wireless anqp-frag-size <100-1500>

service wireless ap650 legacy-auto-update-image <FILE>

service wireless client tx-deauth on-radarr-detect

service wireless cred-cache-sync [full|interval <30-864000>|never|partial]

service wireless test [max-rate|max-retries|min-rate]

service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24,36,48,54,mcs0,
mcs1,..............,mcs23]

service wireless inter-ap-key [0 <WORD>|2 <WORD>|<WORD>]

service wireless noise-immunity

service wireless reconfig-on-rx-stall

service wireless test max-retries <0-15>

service wireless wispe-controller-port <1-65535>

service show cli
The following command is specific to the NX45XX and NX65XX series service platform:

```text
service fast-switching
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service cluster master-election immediate</code></td>
<td>Initiates and completes cluster master election as soon as just one cluster member comes on and is active. This option is disabled by default.</td>
</tr>
<tr>
<td><code>service critical-resource port-mode-source-ip &lt;IP&gt;</code></td>
<td>Hard codes a source IP for critical resource management. The default is 0.0.0.0.</td>
</tr>
<tr>
<td>`service enable [l2tpv3</td>
<td>pppoe</td>
</tr>
<tr>
<td><code>service enable l2tpv3</code></td>
<td>Enables L2TPv3 on this profile. This feature is not supported on AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, and NX9000 model devices.</td>
</tr>
<tr>
<td><code>service enable pppoe</code></td>
<td>Enables PPPoE features. When executed on a device, enables PPPoE on the logged device. When executed on a profile, enables PPPoE on all devices using that profile.</td>
</tr>
<tr>
<td><code>service enable radiusd</code></td>
<td>Enables RADIUS features. When executed on a device, enables RADIUS on the logged device. When executed on a profile, enables RADIUS on all devices using that profile.</td>
</tr>
<tr>
<td><code>service global-association-list blacklist-interval &lt;1-65535&gt;</code></td>
<td>Configures the period for which a client is blacklisted. A client is considered blacklisted after being denied access by the server.</td>
</tr>
<tr>
<td><code>lldp loop-detection</code></td>
<td>Enables network loop detection via LLDP. This option is disabled by default.</td>
</tr>
<tr>
<td><code>service memory kernel decrease</code></td>
<td>Enables reduction in kernel memory usage. When enabled, firewall flows are reduced by 75% resulting in reduced kernel memory usage. A reboot is required for the option to take effect.</td>
</tr>
<tr>
<td>`service meshpoint loop-prevention-port [&lt;L2-INTERFACE-NAME&gt;</td>
<td>ge &lt;1-4&gt;]&lt;L2-INTERFACE-NAME&gt;`</td>
</tr>
<tr>
<td><code>meshpoint loop-prevention-port</code></td>
<td>Limits meshpoint loop prevention on a specified Ethernet interface.</td>
</tr>
<tr>
<td><code>&lt;L2-INTERFACE-NAME&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>pm sys-restart</code></td>
<td>Enables the process monitor (PM) to restart the system when a process fails. The option is enabled by default.</td>
</tr>
<tr>
<td>`power-config [3af-out</td>
<td>force-3at]`</td>
</tr>
<tr>
<td><code>power-config force-3at</code></td>
<td>Disables LLDP negotiation and forces 802.3at power configuration. This option is disabled by default.</td>
</tr>
<tr>
<td><code>radius dynamic-authorization additional-port &lt;1-65535&gt;</code></td>
<td>Configures an additional UDP port used by the device to listen for dynamic authorization messages. The Cisco Identity Services Engine (ISE) server uses port 1700.</td>
</tr>
<tr>
<td><code>remote-config apply-delay &lt;0-600&gt;</code></td>
<td>Delays configuration of a remote device (after it becomes active) by the specified time period. The default is 0 seconds.</td>
</tr>
<tr>
<td><code>rss-timeout &lt;0-86400&gt;</code></td>
<td>Configures the duration, in seconds, for which an adopted access point will continue to provide wireless functions even after losing controller adoption. The default is 300 seconds.</td>
</tr>
<tr>
<td><code>watchdog</code></td>
<td>Enables the watchdog. This feature is enabled by default. Enabling the watchdog option implements heartbeat messages to ensure other associated devices are up and running and capable of effectively inter-operating with the controller.</td>
</tr>
<tr>
<td><code>wireless anqp-frag-always</code></td>
<td>Enables fragmentation of all ANQP packets. This option is disabled by default.</td>
</tr>
<tr>
<td><code>wireless anqp-frag-size &lt;100-1500&gt;</code></td>
<td>Configures the ANQP packet fragment size. The default is 1200.</td>
</tr>
</tbody>
</table>
### service wireless ap650 legacy-auto-update-image <FILE>
- **Invokes AP650 related service commands**
- **legacu-auto-update-image <FILE>**
  - Configures the AP650 image file details, such as location and file name
  - `<FILE>` – Provides the path and name of the AP650 image file (for example, flash:/ap.img)

### service wireless client tx-deauth on-radar-detection
- **Configures wireless client and stations related settings**
- **tx-deauth on-radar-detection**
  - Enables access points to transmit deauth to clients when changing channels on radar detection. This option is enabled by default.

### service wireless cred-cache-sync [full|interval <30-864000>|never|partial]
- **Configures the credential cache’s synchronization parameters.**
  - The parameters are full, interval, never, and partial.
  - **full**
    - Enables synchronization of all credential cache entries
  - **interval <30-864000>**
    - Sets the interval, in seconds, at which the credential cache is synchronized
    - `<30-864000>` – Specify a value from 30 - 864000 seconds. The default is 1200 seconds.
  - **never**
    - Disables credential cache entry synchronization for all associated clients other than roaming clients. This is the default setting.
  - **partial**
    - Enables partial synchronization of parameters for associated clients, with credential cache close to aging out

### service wireless inter-ap-key [0 | 2 | <WORD>]
- **Configure encryption key used for securing inter-ap messages.**
  - This option is disabled by default.
  - **[0 | 2 | <WORD>]**
    - Specify a clear text or encrypted key.

### service wireless noise-immunity
- **Polls for status and reconfigures radio in case of receive stall.**
  - This option is enabled by default.

### service wireless reconfig-on-rx-stall
- **Enables noise immunity on the radio**

### service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24,36,48,54,mcs0,mcs1,.........mcs23]
- **Configures the serviceability parameters used for testing**
  - **[max-rate|min-rate]**
    - Configures the maximum and minimum data rates for clients using rate-scaling. The 'max-rate' and 'min-rate' options are disabled by default.
  - **[1,2,5.5,....mcs23]**
    - Select the maximum and minimum data rates applicable.
**Profiles 7-439**

- **service wireless test max-retries <0-15>**

<table>
<thead>
<tr>
<th>wireless test</th>
<th>Configures the serviceability parameters used for testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-retries &lt;0-15&gt;</td>
<td>Configures the maximum number of retries per packet from 0 - 15. The default is 0.</td>
</tr>
</tbody>
</table>

- **service wireless wispe-controller-port <1-65535>**

<table>
<thead>
<tr>
<th>wispe-controller-port &lt;1-65535&gt;</th>
<th>Resets the <em>Wireless Switch Protocol Enhanced</em> (WISPe) controller port. This is the UDP port used to listen for WISPe.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Specify a value from 1 - 65535. The default is 24756.</td>
</tr>
</tbody>
</table>

- **service show cli**

<table>
<thead>
<tr>
<th>show cli</th>
<th>Displays running system configuration details</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli – Displays the CLI tree of the current mode</td>
<td></td>
</tr>
</tbody>
</table>

- **service fast-switching**

<table>
<thead>
<tr>
<th>fast-switching</th>
<th>Enables fast switching of packets in the hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the <em>no &gt; service &gt; fast-switching</em> command to disable this feature.</td>
<td></td>
</tr>
<tr>
<td>Fast switching can be enabled and disabled on the NX45XX and NX65XX series service platform.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs7000-37FABE(config-profile-testrfs7000)#service radius dynamic-authorization additional-port 1700
rfs7000-37FABE(config-profile-testrfs7000)#show context
profile rfs7000 test
  service radius dynamic-authorization additional-port 1700
  no autoinstall configuration
  no autoinstall firmware
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  --More--
```

**Related Commands**

- **no** Removes or resets service command parameters
7.1.76 slot

Profile Config Commands

Assigns a Peripheral Component Interconnect expansion (PCIe) slot for Team-URC VM or WiNG support. The NX45XX and NX65XX series service platforms support an optional NX expansion module for modular WAN and Telephony Gateway support. The NX Series Expansion Module kit (KT-NXMODC-01) allows for the installation and implementation of up to four PCIe cards. The Expansion Module kit can be installed in NX4500, NX4524, NX6500 or NX6524 model service platforms.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

```
slot <1-4>
```

Parameters

- slot <1-4>

<table>
<thead>
<tr>
<th>slot &lt;1-4&gt;</th>
<th>Enables assignment of PCIe slots for TEAM-Centro or WiNG support. You can also assign the selected slot to any other VM.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-4&gt; – Select the slot from 1 - 4. The command selects the slot and enters its configuration mode.</td>
</tr>
<tr>
<td></td>
<td>In the slot configuration mode, do the following:</td>
</tr>
<tr>
<td></td>
<td>• assign – Assigns the selected slot to either TEAM-Centro VM, WiNG, or other VM support</td>
</tr>
<tr>
<td></td>
<td>• team-centro – Assigns the selected slot to TEAM-Centro VM (IP PBX)</td>
</tr>
<tr>
<td></td>
<td>• wing – Assigns the selected slot to WiNG</td>
</tr>
<tr>
<td></td>
<td>• other – Assigns the selected slot to other VM</td>
</tr>
</tbody>
</table>

**Note:** The show > slot command displays slots and their assignment details (type and status). Use the no > assign command to override the slot assignment configured.

Examples

```
nx4500-5CFA2B(config-profile-testNX45XX)#slot 1
nx4500-5CFA2B(config-profile-testNX45XX-slot-1)#
```

```
nx4500-5CFA2B(config-profile-testNX45XX-slot-1)#?
```

Slot Mode commands:
- assign Assign the slot
- no Negate a command or set its defaults
- shutdown Disable the slot
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

```
nx4500-5CFA2B(config-profile-testNX45XX-slot-1)#
nx4500-5CFA2B(config-profile-testNX45XX-slot-1)#assign team-centro
```
nx4500-5CFA2B(config-profile testNX45XX-slot-1)#show context
  slot 1
    assign team-centro
    nx4500-5CFA2B(config-profile testNX45XX-slot-1)#

nx4500-5CFA2B(config-device B4-C7-99-5C-FA-2B-slot-1)#show slot
-----------------------------------
SLOT TYPE | MODULE | STATUS
-----------------------------------
1         | []     | team-centro Enabled
2         | []     | wing Enabled
3         | []     | wing Enabled
4         | []     | wing Enabled
-----------------------------------

nx4500-5CFA2B(config-device B4-C7-99-5C-FA-2B-slot-1)#

nx4500-5CFA2B(config-profile testNX45XX-slot-1)#no assign

nx4500-5CFA2B(config-profile testNX45XX-slot-1)#show context
  slot 1
  nx4500-5CFA2B(config-profile testNX45XX-slot-1)#

Use the shutdown option to shut down the selected slot.

nx4500-5CFA2B(config-profile testNX45XX-slot-1)#shutdown

Related Commands

| no                      | Removes the PCI expansion slot assignment for Team-URC VM or WiNG support |
7.2 Device Config Commands

- **PROFILES**

  Use the (config) instance to configure device specific parameters

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#<DEVICE-TYPE> <MAC>
<DEVICE>(config-device-<MAC>)#?
```

Device Mode commands:

- **adopter-auto-provisioning-policy-lookup**
  Use centralized auto-provisioning policy when adopted by another controller

- **adoption**
  Adoption configuration

- **adoption-site**
  Set system's adoption site

- **alias**
  Alias

- **application-policy**
  Application Policy configuration

- **area**
  Set name of area where the system is located?

- **arp**
  Address Resolution Protocol (ARP)

- **auto-learn-staging-config**
  Enable learning network configuration of the devices that come for adoption

- **autogen-uniqueid**
  Autogenerate a unique id

- **autoinstall**
  Autoinstall settings

- **bluetooth-detection**
  Detect Bluetooth devices using the Bluetooth USB module

- **bridge**
  Ethernet bridge

- **captive-portal**
  Captive portal

- **cdp**
  Cisco Discovery Protocol

- **channel-list**
  Configure channel list to be advertised to wireless clients

- **cluster**
  Cluster configuration

- **configuration-persistence**
  Enable persistence of configuration across reloads (startup config file)

- **contact**
  Configure the contact

- **controller**
  WLAN controller configuration

- **country-code**
  Configure the country of operation

- **critical-resource**
  Critical Resource

- **crypto**
  Encryption related commands

- **database-backup**
  Scheduled Database Backup

- **device-upgrade**
  Device firmware upgrade

- **dot1x**
  802.1X

- **dpi**
  Enable Deep-Packet-Inspection (Application Assurance)

- **dscp-mapping**
  Configure IP DSCP to 802.1p priority mapping for untagged frames

- **email-notification**
  Email notification configuration

- **enforce-version**
  Check the firmware versions of devices before interoperating

- **environmental-sensor**
  Environmental Sensors Configuration

- **events**
  System event messages

- **export**
  Export a file

- **file-sync**
  File sync between controller and adoptees

- **floor**
  Set the floor within a area where the system is located

- **geo-coordinates**
  Configure geo coordinates for this device

- **gre**
  GRE protocol

- **hostname**
  Set system's network name

- **http-analyze**
  Specify HTTP-Analysis configuration

- **interface**
  Select an interface to configure

- **ip**
  Internet Protocol (IP)

- **ipv6**
  Internet Protocol version 6 (IPv6)

- **ldtpv3**
  L2tpv3 protocol

- **l3e-lite-table**
  L3e lite Table
layout-coordinates
led
led-timeout
legacy-auto-downgrade
legacy-auto-update
license
lldp
load-balancing
location
logging
mac-address-table
mac-auth
mac-name
memory-profile
meshpoint-device
meshpoint-monitor-interval
min-misconfiguration-recovery-time
mint
mirror
misconfiguration-recovery-time
neighbor-inactivity-timeout
neighbor-info-interval
no
noc
ntp
offline-duration
override-wlan
power-config
preferred-controller-group
preferred-tunnel-controller
radius
raid
remove-override
rf-domain-manager
router
rsa-key
sensor-server
slot
spanning-tree
traffic-class-mapping
traffic-shape
trustpoint
timezone
tunnel-controller

Configure layout coordinates for this device
Turn LEDs on/off on the device
Configure the time for the led to turn off after the last radio state change
Enable device firmware to auto downgrade when other legacy devices are detected
Auto upgrade of legacy devices
License management command
Link Layer Discovery Protocol
Configure load balancing parameter
Configure the location
Modify message logging facilities
MAC Address Table
802.1X
Configure MAC address to name mappings
Memory profile to be used on the device
Configure meshpoint device parameters
Configure meshpoint monitoring interval
Check controller connectivity after configuration is received
MiNT protocol
Mirroring
Check controller connectivity after configuration is received
Configure neighbor inactivity timeout
Configure neighbor information exchange interval
Negate a command or set its defaults
Configure the noc related setting
Ntp server A.B.C.D
Set duration for which a device remains unadopted before it generates offline event
Configure RF Domain level overrides for wlan
Configure power mode
Controller group this system will prefer for adoption
Tunnel Controller Name this system will prefer for tunneling extended vlan traffic
Configure device-level radius authentication parameters
RAID
Remove configuration item override from the device (so profile value takes effect)
RF Domain Manager
Dynamic routing
Assign a RSA key to a service
AirDefense sensor server configuration
PCI expansion Slot
Spanning tree
Configure IPv6 traffic class to 802.1p priority mapping for untagged frames
Traffic shaping
Assign a trustpoint to a service
Configure the timezone
Tunnel Controller group this
The following table summarizes device configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopter-auto-provisioning-policy-lookup</td>
<td>Enables the use of a centralized auto provisioning policy on this device</td>
<td>page 7-11</td>
</tr>
<tr>
<td>adoption</td>
<td>Configures a minimum and maximum delay time in the initiation of the device adoption process</td>
<td>page 7-12</td>
</tr>
<tr>
<td>adoption-site</td>
<td>Sets the device’s adoption site name</td>
<td>page 7-449</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, VLAN, and service aliases on a device</td>
<td>page 7-13</td>
</tr>
<tr>
<td>application-policy</td>
<td>Associates a RADIUS server provided application policy with this device. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane.</td>
<td>page 7-20</td>
</tr>
<tr>
<td>area</td>
<td>Sets the name of area where the system is deployed</td>
<td>page 7-450</td>
</tr>
<tr>
<td>arp</td>
<td>Configures ARP parameters</td>
<td>page 7-22</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enables automatic recognition of devices pending adoption</td>
<td>page 7-24</td>
</tr>
<tr>
<td>autogen-uniqueid</td>
<td>When executed in the device configuration mode, this command generates a unique ID for the logged device</td>
<td>page 7-25</td>
</tr>
<tr>
<td>autoinstall</td>
<td>Autostarts firmware image and configuration setup parameters</td>
<td>page 7-27</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures Ethernet Bridging parameters</td>
<td>page 7-29</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures captive portal advanced Web page upload on this profile</td>
<td>page 7-55</td>
</tr>
<tr>
<td>cdp</td>
<td>Operates CDP on the device</td>
<td>page 7-56</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures channel list advertised to wireless clients</td>
<td>page 7-451</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>cluster</td>
<td>Sets cluster configuration</td>
<td>page 7-57</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enables configuration persistence across reloads</td>
<td>page 7-60</td>
</tr>
<tr>
<td>contact</td>
<td>Sets contact information</td>
<td>page 7-452</td>
</tr>
<tr>
<td>controller</td>
<td>Configures a WLAN's wireless controller or service platform</td>
<td>page 7-61</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures wireless controller or service platform's country code</td>
<td>page 7-453</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Monitors user configured IP addresses and logs their status</td>
<td>page 7-65</td>
</tr>
<tr>
<td>crypto</td>
<td>Configures data encryption protocols and settings</td>
<td>page 7-72</td>
</tr>
<tr>
<td>database-backup</td>
<td>Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server. When applied to devices, this profile will enable the back up of the specified database.</td>
<td>page 7-133</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings on this device</td>
<td>page 7-134</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures 802.1x standard authentication controls</td>
<td>page 7-136</td>
</tr>
<tr>
<td>dpi</td>
<td>Enables Deep Packet Inspection (DPI) on this device</td>
<td>page 7-138</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configures IP Differentiated Services Code Point (DSCP) to 802.1p priority mapping for untagged frames</td>
<td>page 7-140</td>
</tr>
<tr>
<td>email-notification</td>
<td>Configures e-mail notification settings</td>
<td>page 7-141</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Checks the device firmware version before attempting connection</td>
<td>page 7-143</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configure its settings.</td>
<td>page 7-144</td>
</tr>
<tr>
<td>events</td>
<td>Enables system event message generation and forwarding</td>
<td>page 7-146</td>
</tr>
<tr>
<td>export</td>
<td>Enables export of startup.log file after every boot</td>
<td>page 7-147</td>
</tr>
<tr>
<td>file-sync</td>
<td>Configures parameters enabling synching of PKCS#12 certificate between the staging-controller and adoptee AP6522/AP6562 client bridges</td>
<td>page 7-148</td>
</tr>
<tr>
<td>floor</td>
<td>Sets the floor name where the system is located</td>
<td>page 7-149</td>
</tr>
<tr>
<td>geo-coordinates</td>
<td>Configures the geographic coordinates for this device</td>
<td>page 7-455</td>
</tr>
<tr>
<td>gre</td>
<td>Enables GRE tunneling on this device</td>
<td>page 7-151</td>
</tr>
<tr>
<td>hostname</td>
<td>Sets a system's network name</td>
<td>page 7-456</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enables HTTP analysis on this device</td>
<td>page 7-162</td>
</tr>
<tr>
<td>interface</td>
<td>Selects an interface to configure</td>
<td>page 7-167</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IPv4 components</td>
<td>page 7-348</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures IPv6 components</td>
<td>page 7-357</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Defines the Layer 2 Tunnel Protocol (L2TP) protocol for tunneling Layer 2 payloads using Virtual Private Networks (VPNs)</td>
<td>page 7-361</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>Configures L3e Lite Table with this profile</td>
<td>page 7-363</td>
</tr>
<tr>
<td>layout-coordinates</td>
<td>Configures layout coordinates</td>
<td>page 7-457</td>
</tr>
<tr>
<td>led</td>
<td>Turns LEDs on or off</td>
<td>page 7-364</td>
</tr>
<tr>
<td>led-timeout</td>
<td>Configures the LED-timeout timer in the device or profile configuration mode</td>
<td>page 7-365</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Enables legacy device firmware to auto downgrade</td>
<td>page 7-367</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto updates AP650 and AP71XX legacy device firmware</td>
<td>page 7-368</td>
</tr>
<tr>
<td>license</td>
<td>Adds device feature licenses</td>
<td>page 7-458</td>
</tr>
<tr>
<td>llpd</td>
<td>Configures Link Layer Discovery Protocol (LLDP) settings for this device</td>
<td>page 7-369</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configures load balancing parameters.</td>
<td>page 7-371</td>
</tr>
<tr>
<td>location</td>
<td>Configures the system’s location (place of deployment)</td>
<td>page 7-460</td>
</tr>
<tr>
<td>logging</td>
<td>Enables message logging</td>
<td>page 7-376</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Configures the MAC address table</td>
<td>page 7-378</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables 802.1x authentication of hosts on this device</td>
<td>page 7-380</td>
</tr>
<tr>
<td>mac-name</td>
<td>Configures MAC address to device name mappings</td>
<td>page 7-461</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Configures memory profile used on the device</td>
<td>page 7-383</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configures meshpoint device parameters</td>
<td>page 7-384</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configures meshpoint monitoring interval</td>
<td>page 7-385</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Configures the minimum device connectivity verification time</td>
<td>page 7-386</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol settings</td>
<td>page 7-387</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Verifies device connectivity after a configuration is received</td>
<td>page 7-394</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configures neighbor inactivity timeout value</td>
<td>page 7-395</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configures the neighbor information exchange interval</td>
<td>page 7-396</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or resets values to their default settings</td>
<td>page 7-462</td>
</tr>
<tr>
<td>noc</td>
<td>Configures NOC settings</td>
<td>page 7-399</td>
</tr>
<tr>
<td>ntp</td>
<td>Configures NTP server settings</td>
<td>page 7-400</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>offline-duration</td>
<td>Sets the duration, in minutes, for which a device remains unadopted before it generates offline event</td>
<td>page 7-403</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configures WLAN RF Domain level overrides on the logged device</td>
<td>page 7-463</td>
</tr>
<tr>
<td>power-config</td>
<td>Configures power mode features</td>
<td>page 7-404</td>
</tr>
<tr>
<td>preferred-controller-group</td>
<td>Specifies the wireless controller or service platform group the system prefers for adoption</td>
<td>page 7-406</td>
</tr>
<tr>
<td>preferred-tunnel-controller</td>
<td>Configures the tunnel wireless controller or service platform preferred by the system for tunneling extended VLAN traffic</td>
<td>page 7-407</td>
</tr>
<tr>
<td>radius</td>
<td>Configures device-level RADIUS authentication parameters</td>
<td>page 7-408</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides</td>
<td>page 7-465</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Enables the RF Domain manager</td>
<td>page 7-409</td>
</tr>
<tr>
<td>router</td>
<td>Configures dynamic router protocol settings.</td>
<td>page 7-410</td>
</tr>
<tr>
<td>rsa-key</td>
<td>Assigns a RSA key to SSH</td>
<td>page 7-467</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server</td>
<td>page 7-468</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Enables spanning tree commands on the logged device</td>
<td>page 7-412</td>
</tr>
<tr>
<td>traffic-class-mapping</td>
<td>Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority</td>
<td>page 7-415</td>
</tr>
<tr>
<td>traffic-shape</td>
<td>Enables traffic shaping and configures traffic shaping parameters on this device</td>
<td>page 7-417</td>
</tr>
<tr>
<td>trustpoint (device-config-mode)</td>
<td>Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server etc.</td>
<td>page 7-470</td>
</tr>
<tr>
<td>timezone</td>
<td>Configures wireless controller or service platform’s time zone settings</td>
<td>page 7-469</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Configures the tunneled WLAN (extended VLAN) wireless controller or service platform’s name</td>
<td>page 7-424</td>
</tr>
<tr>
<td>use</td>
<td>Associates different policies and settings with this device</td>
<td>page 7-425</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configures VRRP group settings</td>
<td>page 7-430</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>Publishes interface via OSPF or BGP based on Virtual Router Redundancy Protocol (VRRP) status</td>
<td>page 7-434</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enables support for 802.11 WEP shared key authentication</td>
<td>page 7-435</td>
</tr>
<tr>
<td>mirror</td>
<td>Enables port mirroring on GE ports. This command is supported only on the NX4524 and NX6524 series service platforms.</td>
<td>page 7-472</td>
</tr>
<tr>
<td>raid</td>
<td>Enables alarm on the array. This command is supported only on the NX9500 series service platform.</td>
<td>page 7-474</td>
</tr>
<tr>
<td>slot</td>
<td>Assigns a physical slot for running Team-URC VM on this profile/device. This feature is support only on the NX45XX and NX65XX series service platforms.</td>
<td>page 7-441</td>
</tr>
</tbody>
</table>
7.2.1 adoption-site

- **Device Config Commands**

Sets the device's adoption site name

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
adoption-site <SITE-NAME>
```

**Parameters**

- `adoption-site <SITE-NAME>`

<table>
<thead>
<tr>
<th>adoption-site &lt;SITE-NAME&gt;</th>
<th>Sets the device's adoption site name</th>
</tr>
</thead>
</table>

**Examples**

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#adoption-site SanJoseMainOffice
```

**Related Commands**

<table>
<thead>
<tr>
<th>no</th>
<th>Disables or reverts settings to their default</th>
</tr>
</thead>
</table>
### 7.2.2 area

**Device Config Commands**

Sets the physical area where the device (controller, service platform, or access point) is deployed. This can be a building, region, campus or other area that describes the deployment location of the device. Assigning an area name is helpful when grouping devices in RF Domains and profiles, as devices in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`area <AREA-NAME>`

**Parameters**

- `area <AREA-NAME>`

**Examples**

```
area RMZEcoSpace
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#area RMZEcoSpace
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
```

```
ap71xx 00-04-96-4A-A7-08
```

```
use profile default-ap71xx
```

```
use rf-domain default
```

```
hostname ap7131-4AA708
```

```
area RMZEcospace
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables or reverts settings to their default</td>
</tr>
</tbody>
</table>
7.2.3 channel-list

Device Config Commands

Configures the channel list advertised to wireless clients

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

channel-list [2.4GHz|5GHz|dynamic]

channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]

Parameters

- channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]

<table>
<thead>
<tr>
<th>channel-list</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2.4GHz <CHANNEL-LIST> | Configures the channel list advertised by radios operating in 2.4 GHz  
  - <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens. |
| 5GHz <CHANNEL-LIST> | Configures the channel list advertised by radios operating in 5.0 GHz  
  - <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens. |
| dynamic | Enables dynamic (neighboring access point based) update of configured channel list |

Examples

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#channel-list 2.4GHz 1,2

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
  use profile default-ap71lx
  use rf-domain default
  hostname ap7131-4AA708
  area RMZEcospace
channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

Related Commands

- no  | Resets the channel list configuration |
7.2.4 contact

▸ Device Config Commands

Defines an administrative contact for a deployed device (controller, service platform, or access point)

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
contact <WORD>
```

Parameters

- `contact <WORD>`

Examples

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#contact Bob+1-631-738-5200
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
  ap71xx 00-04-96-4A-A7-08
    use profile default-ap71xx
    use rf-domain default
    hostname ap7131-4AA708
    area RMZEcospac
    contact Bob+1-631-738-5200
    channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

| **no** | Resets the administrative contact name |
7.2.5 country-code

Device Config Commands

Defines the two digit country code for legal device deployment

Configuring the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
country-code <WORD>

Parameters
- country-code <COUNTRY-CODE>

<table>
<thead>
<tr>
<th>country-code &lt;COUNTRY-CODE&gt;</th>
<th>Defines the two digit country code for legal device deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;COUNTRY-CODE&gt; – Specify the two letter ISO-3166 country code.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#country-code us

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
  use profile default-ap71xx
  use rf-domain default
  hostname ap7131-4AA708
  area RMZEcospace
  contact Bob+1-631-738-5200
country-code us
  channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

Related Commands
- no | Removes the configured country code
7.2.6 floor

- **Device Config Commands**

Sets the building floor name representative of the location within the area or building the device (controller, service platform, or access point) is physically deployed. Assigning a building floor name is helpful when grouping devices in RF Domains and profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
floor <FLOOR-NAME> <1-4094>
```

**Parameters**

- `floor <FLOOR-NAME> <1-4094>`

**Examples**

```plaintext
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#floor 5thfloor

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
use profile default-ap71xx
use rf-domain default
hostname ap7131-4AA708
area RMZEcospae
floor 5thfloor
contact Bob+1-631-738-5200
country-code us
channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

- `no` Removes device’s location floor name
### 7.2.7 geo-coordinates

#### Device Config Commands

Configures the geographic coordinates for this device. Specifies the exact location of this device in terms of latitude and longitude coordinates.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

#### Parameters

- **geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>**

#### Examples

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#geo-coordinates -90.0000 166.0000
rfs4000-229D58(config-device-00-23-68-22-9D-58)#show context
rfs4000 00-23-68-22-9D-58
use profile default-rfs4000
use rf-domain default
hostname rfs4000-229D58
license AP DEFAULT-6AP-LICENSE
license ADSEC DEFAULT-ADV-SEC-LICENSE
ip default-gateway 192.168.13.2
ip default-gateway priority static-route 20
interface ge1
  switchport mode access
  switchport access vlan 1
interface vlan1
  ip address 192.168.13.9/24
  ip address 192.168.0.1/24 secondary
  ip dhcp client request options all
  use client-identity-group ClientIdentityGroup
logging on
logging console warnings
logging buffered warnings
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes device’s geographic coordinates</td>
</tr>
</tbody>
</table>
7.2.8 **hostname**

- **Device Config Commands**

Sets the system’s network name

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

hostname <WORD>

**Parameters**

- hostname <WORD>

  | hostname <WORD> | Sets the name of the managing wireless controller, service platform, or access point. This name is displayed when accessed from any network.

**Examples**

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#hostname TechPubAP7131

The hostname has changed from ‘ap7131-4AA708’ to ‘TechPubAP7131’

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
  ap71xx 00-04-96-4A-A7-08
  use profile default-ap71xx
  use rf-domain default
hostname TechPubAP7131
area RMZEcospace
floor 5thfloor
contact Bob+1-631-738-5200
country-code us
channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

**Related Commands**

| no | Removes device’s hostname |
7.2.9 layout-coordinates

Device Config Commands

Configures X and Y layout coordinates for the device

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>

Parameters
- layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>

<table>
<thead>
<tr>
<th>layout-coordinates</th>
<th>Configures X and Y layout coordinates for the device</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;-4096.0-4096.0&gt;</td>
<td>Specify the X coordinate from -4096 - 4096.0</td>
</tr>
<tr>
<td>&lt;-4096.0-4096.0&gt;</td>
<td>Specify the Y coordinate from -4096 - 4096.0</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#layout-coordinates 1.0 2.0

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
  use profile default-ap71xx
  use rf-domain default
  hostname TechPubAP7131
  area RMZEcospaсe
  floor 5thfloor
  layout-coordinates 1.0 2.0
  contact Bob+1-631-738-5200
  country-code us
  channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

Related Commands
- no

Removes device’s layout co-ordinates
7.2.10 *license*

*Device Config Commands*

Adds a license pack on the device for the specified feature (AP/AAP/ADSEC/HTANLT/SMART-CACHE/WEBF)

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center (NOC)* controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

The NOC controllers and/or site controllers can both have license packs installed. Adoption of APs by the NOC and site controllers depends on the number of licenses available on each of these controllers.

The NOC controllers and/or site controllers can both have license packs installed. When a AP is adopted by a site controller, the site controller pushes a license on to the AP. The various possible scenarios are:

- **AP licenses installed only on NOC controller:**
  The NOC controller provides the site controllers with AP licenses, ensuring that per platform limits are not exceeded.

- **AP licenses installed on site controller:**
  The site controller uses its installed licenses, and then asks the NOC controller for additional licenses in case of a shortage.
  In a hierarchical and centrally managed network, the NOC controller can pull unused AP licenses from site controllers and relocate to other site controllers when required.

- **AP licenses installed on any member of a site cluster:**
  The site controller shares installed and borrowed (from the NOC) licenses with other controllers within a site cluster.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`license <WORD> <LICENSE-KEY>`

**Parameters**

- `license <WORD> <LICENSE-KEY>`

<table>
<thead>
<tr>
<th><code>&lt;WORD&gt;</code></th>
<th>Specify the feature name (AP/AAP/ADSEC/HTANLT/SMART-CACHE/WEBF/NSIGHT) for which license is added</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> NSight is supported only on NX9500, NX9510, and NX9600 model service platforms.</td>
<td></td>
</tr>
</tbody>
</table>

| `<LICENSE-KEY>` | Specify the license key |
Examples

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#license ap aplicensekey@123

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
use profile default-ap71xx
use rf-domain default
hostname TechPubAP7131
floor 5thfloor
layout-coordinates 1.0 2.0
license AP aplicensekey@1234 aplicensekey@123
location SanJose
no contact
country-code us
channel-list 2.4GHz 1,2
mac-name 00-04-96-4A-A7-08 5.8TestAP
neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

nx6524-858126(config-device-5C-0E-8B-85-81-26)#license ?
  WORD Feature name (AP/AAP/ADSEC/HTANLT/SMART-CACHE/WEBF) for which license is to be added

nx6524-858126(config-device-5C-0E-8B-85-81-26)#license SMART-CACHE
29bedfa30cf4a5bcd20cd8815e00c948df26b14e8346ef6f9e884832a7a49b349e6938f63ef653

nx6524-858126(config-device-5C-0E-8B-85-81-26)#commit

nx6524-858126(config-device-5C-0E-8B-85-81-26)#show licenses
Serial Number : 1118520500065

Device Licenses:
  AP-LICENSE
    String : 29bedfa30cf4a5bc60c732a20e39f728df26b14e8346ef6739f3ee281691d10246de8a1e439131

  HOTSPOT-ANALYTICS
    String : 29bedfa30cf4a5bc63ad26e814f39d9df26b14e8346ef6f429383a6d51d659e6938f63ef653

  SMART-CACHE
    String : 29bedfa30cf4a5bcd20cd8815e00c948df26b14e8346ef6f9e884832a7a49b349e6938f63ef653

--More--
nx6524-858126(config-device-5C-0E-8B-85-81-26)#
# 7.2.11 location

▲ **Device Config Commands**

Sets the location where a managed device (controller, service platform, or access point) is deployed. This is the location of the device with respect to the RF Domain it belongs.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`location <WORD>`

**Parameters**

- `location <WORD>`

**Examples**

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#location SanJose
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
    ap71xx 00-04-96-4A-A7-08
    use profile default-ap71xx
    use rf-domain default
    hostname TechPubAP7131
    area RMZEcospacex
    floor 5thfloor
    layout-coordinates 1.0 2.0
    location SanJose
    contact Bob+1-631-738-5200
    country-code us
    channel-list 2.4GHz 1,2
    rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a managed device’s location</td>
</tr>
</tbody>
</table>
### 7.2.12 `mac-name`

#### Device Config Commands

Configures a client name to MAC address mapping. Use this command to assign a user-friendly name to the device (controller, service platform, or access point) and map it to the device’s MAC address.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
mac-name <MAC> <NAME>
```

#### Parameters

- **mac-name <MAC> <NAME>**
  - `<MAC>` — Specify the device’s MAC address.
  - `<NAME>` — Specify the ‘friendly’ name used for the specified MAC address. This is the name used in events and statistics logs.

#### Examples

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#mac-name 00-04-96-4A-A7-08 5.8TestAP
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
use profile default-ap71xx
use rf-domain default
hostname TechPubAP7131
area RMZEcospace
floor 5thfloor
layout-coordinates 1.0 2.0
location SanJose
contact Bob+1-631-738-5200
country-code us
channel-list 2.4GHz 1,2
mac-name 00-04-96-4A-A7-08 5.8TestAP
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the device’s friendly name to MAC address mapping</td>
</tr>
</tbody>
</table>
7.2.13 **no**

*Device Config Commands*

Negates a command or resets values to their default

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

\[ \text{no } \text{[adopter-auto-provisioning-policy-lookup|adoption-site|alias|application-policy|area|arp|auto-learn-staging-config|autoinstall|bridge|captive-portal|cdp|channel-list|cluster|configuration-persistence|contact|controller|country-code|critical-resource|crypto|database-backup|device-upgrade|dot1x|dpi|dscp-mapping|email-notification|environmental-sensor|events|export|file-sync|floor|geo-coordinates|gre|hostname|http-analyze|interface|ip|ipv6|l2tpv3|l3-lite-table|layout-coordinates|led|led-timeout|legacy-auto-downgrade|legacy-auto-update|license|lldp|load-balancing|location|logging|mac-address-table|mac-auth|mac-name|memory-profile|meshpoint-device|meshpoint-monitor-interval|min-misconfiguration-recovery-time|mint|mirror|misconfiguration-recovery-time|noc|ntp|offline-duration|override-wlan|power-config|preferred-controller-group|preferred-tunnel-controller|radius|raid|rf-domain-manager|router|rsa-key|sensor-server|slot|spanning-tree|timezone|traffic-class-mapping|traffic-shape|trustpoint|tunnel-controller|use|vrrp|vrrp-state-check|wep-shared-key-auth|service] } \]

**Parameters**

- **no <PARAMETERS>**

**Usage Guidelines**

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

**Examples**

```
 rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no area
```

```
 rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no contact
```
7.2.14 override-wlan

Configure WLAN's RF Domain level overrides

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

override-wlan <WLAN> [shutdown|ssid|vlan-pool|wep128|wpa-wpa2-psk]
override-wlan <WLAN> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}]
override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]|transmit-key <1-4>]

Parameters

- override-wlan <WLAN> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}]
- override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]|transmit-key <1-4>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WLAN&gt;</td>
<td>Specify the WLAN name.</td>
<td>Configure the following WLAN parameters: SSID, VLAN pool, and WPA-WPA2 key.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the WLAN’s (identified by the &lt;WLAN&gt; keyword) operations on all mapped radios</td>
<td></td>
</tr>
<tr>
<td>SSID &lt;SSID&gt;</td>
<td>Configures the WLAN’s Service Set Identifier (SSID)</td>
<td></td>
</tr>
<tr>
<td>vlan-pool &lt;1-4094&gt;</td>
<td>Configures a pool of VLANs for the selected WLAN</td>
<td></td>
</tr>
<tr>
<td>{limit &lt;0-8192&gt;}</td>
<td>• &lt;SSID&gt; – Specify an SSID ID.</td>
<td></td>
</tr>
<tr>
<td>wpa-wpa2-psk &lt;WORD&gt;</td>
<td>Configures the WLAN WPA-WPA2 key or passphrase for the selected WLAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify a WPA-WPA2 key or passphrase.</td>
<td></td>
</tr>
<tr>
<td>override-wlan &lt;WLAN&gt; wep128 [key &lt;1-4&gt; hex [0&lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]</td>
<td>transmit-key &lt;1-4&gt;</td>
</tr>
</tbody>
</table>
wep128 [key <1-4> hex [0 <WORD>] [2 <WORD>]] transmit-key <1-4>] Configures the WEP128 key for this WLAN, and also enables key transmission

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard. WEP 128 uses a 104 bit key, which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. This results in a level of security and privacy comparable to that of a wired LAN.

- key <1-4> hex – Configures a hexadecimal key (clear text or encrypted) and specifies the key's index.
- 0 <WORD> – Configures a clear text key. Specify a 4 - 32 character pass key.
- 2 <WORD> – Configures an encrypted key. Specify a 4 - 32 character pass key.
- transmit-key <1-4> – Enables transmission of key index. Specify the key index.

Contd...

Note: Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without the required adapters need to use WEP keys manually configured as hexadecimal numbers.

Examples

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#override-wlan test vlan-pool 8
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
  use profile default-ap71xx
  use rf-domain default
  hostname TechPubAP7131
  floor 5thfloor
  layout-coordinates 1.0 2.0
  license AP aplicenseley@1234 aplicensekey@123
  location SanJose
  no contact
  country-code us
  channel-list 2.4GHz 1,2
override-wlan test vlan-pool 8
mac-name 00-04-96-4A-A7-08 5.8TestAP
neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

```
no
```

Removes RF Domain level WLAN overrides
7.2.15 remove-override

Removes device overrides in order to enable profile settings to take effect

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

remove-override <PARAMETERS>

Parameters

- remove-override <PARAMETERS>

| remove-override <PARAMETERS> | Removes settings configured at the device level based on the parameters passed. The profile (applied to the device) settings take effect once the device-level overrides are removed. |

Examples

rfs4000-229D58 (config-device-00-23-68-22-9D-58)#remove-override ?
adopter-auto-provisioning-policy-lookup Use centralized auto-provisioning policy when adopted by another controller
adoption Adoption configuration
alias Alias
application-policy Application Policy configuration
all Remove all overrides for the device
area Reset name of area where the system is located
arp Address Resolution Protocol (ARP)
auto-learn-staging-config Enable learning network configuration of the devices that come for adoption
autogen-uniqueid Autogenerate a unique id
autoinstall Autoinstall settings
bluetooth-detection Detect Bluetooth devices using the Bluetooth USB module
bridge Bridge group commands
captive-portal Captive portal
cdp Cisco Discovery Protocol
cchannel-list Configure a channel list to be advertised to wireless clients
cluster Cluster configuration
cconfiguration-persistence Automatic write of startup configuration file
ccontact The contact
ccontroller WLAN controller configuration
country-code The country of operation
critical-resource Critical Resource
crypto Encryption related commands
device-upgrade Device firmware upgrade
dotix 802.1X
dpi Deep-Packet-Inspection (Application Assurance)
dscp-mapping IP DSCP to 802.1p priority mapping for untagged frames
e-mail-notification Email notification configuration
enforce-version Check the firmware versions of devices before interoperating
environmental-sensor Environmental Sensors Configuration
events System event messages
export                                   Export a file
file-sync                                File sync between controller and adoptees
firewall                                 Enable/Disable firewall
floor                                    Reset name of floor where the system is located
global                                   Remove global overrides for the device but keeps per-interface overrides
gre                                      GRE protocol
interface                                Select an interface to configure
ip                                        Internet Protocol (IP)
ipv6                                      Internet Protocol version 6 (IPv6)
l2tpv3                                    L2tpv3 protocol
l3e-lite-table                           L3e lite Table
led                                       LED on the device
lldp                                      Link Layer Discovery Protocol
location                                  The location
logging                                   Modify message logging facilities
mac-address-table                        MAC Address Table
mac-auth                                  Memory-profile
memory-profile                           Memory-profile
mint                                      MiNT protocol
noc                                       Noc related configuration
ntp                                        Configure NTP
offline-duration                          Duration to mark adopted device as offline
override-wlan                            Overrides for wlans
power-config                              Configure power mode
preferred-controller-group               Controller group this system will prefer for adoption
preferred-tunnel-controller              Tunnel Controller Name this system will prefer for tunneling extended vlan traffic
rf-domain-manager                        RF Domain Manager
router                                    Dynamic routing
routing-policy                            Policy Based Routing Configuration
sensor-server                            AirDefense WIPS sensor server configuration
spanning-tree                            Spanning tree
timezone                                  The timezone
traffic-class-mapping                    IPv6 traffic-class to 802.1p priority mapping for untagged frames
traffic-shape                            Traffic shaping
tunnel-controller                        Tunnel Controller group this controller belongs to
use                                       Set setting to use
vrrp                                      VRRP configuration
service                                   Service Commands

rfs4000-229D58(config-device-00-23-68-22-9D-58)#
## 7.2.16 rsa-key

### Device Config Commands

Assigns an SSH RSA key

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. Secure Shell (SSH) public key authentication can be used by a requesting client to access resources, if properly configured. The RSA key pair must be generated on the client. The public portion of the key pair resides with the controller, service platform, or access point locally, while the private portion remains on a secure area of the client.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9600

### Syntax

`rsa-key ssh <RSA-KEY-NAME>`

### Parameters

- `rsa-key ssh <RSA-KEY-NAME>`

<table>
<thead>
<tr>
<th>rsa-key ssh &lt;RSA-KEY-NAME&gt;</th>
<th>Assigns RSA key to SSH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;RSA-KEY-NAME&gt;</code> – Specifies the RSA key name. The key should be installed using PKI commands in the enable mode.</td>
</tr>
</tbody>
</table>

### Examples

```
    rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#rsa-key ssh rsa-key1

    rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
    ap71xx 00-04-96-4A-A7-08
    use profile default-ap71xx
    use rf-domain default
    hostname TechPubAP7131
    floor 5thfloor
    layout-coordinates 1.0 2.0
    license AP alicensekey@1234 alicensekey@123

    rsa-key ssh rsa-key1
    location SanJose
    no contact
    country-code us
    channel-list 2.4GHz 1,2
    override-wlan test vlan-pool 8
    mac-name 00-04-96-4A-A7-08 5.8TestAP
    neighbor-info-interval 50
    rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

### Related Commands

| no | Removes RSA key from service |
### 7.2.17 sensor-server

*Device Config Commands*

Configures an AirDefense sensor server resource for client terminations and WIPS event logging. This is the server that supports WIPS events on behalf of the controller or service platform.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}  
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor-server &lt;1-3&gt; ip &lt;IP/HOSTNAME&gt; {port [443</td>
<td>&lt;1-65535&gt;]}</td>
</tr>
<tr>
<td>ip &lt;IP/HOSTNAME&gt;</td>
<td>Configures the AirDefense sensor server’s IP address or hostname</td>
</tr>
<tr>
<td>port [443</td>
<td>&lt;1-65535&gt;]</td>
</tr>
<tr>
<td></td>
<td>• 443 – The default port used by the AirDefense server</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Manually sets the port number of the AirDefense server from 1 - 65535</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#sensor-server 1 ip 172.16.10.7
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
  use profile default-ap71xx
  use rf-domain default
  hostname TechPubAP7131
  floor 5thfloor
  layout-coordinates 1.0 2.0
  license AP aplicenseley@1234 aplicensekey@123
  rsa-key ssh rsa-key1
  location SanJose
  no contact
  country-code us
  sensor-server 1 ip 172.16.10.7
  channel-list 2.4GHz 1,2
  override-wlan test vlan-pool 8
  mac-name 00-04-96-4A-A7-08 5.8TestAP
  neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes configured sensor server settings</td>
</tr>
</tbody>
</table>
### 7.2.18 timezone

**Device Config Commands**

Configures device’s timezone

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
timezone <TIMEZONE>
```

**Parameters**

- `timezone <TIMEZONE>`

**Examples**

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#timezone Etc/UTC
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
  use profile default-ap71xx
  use rf-domain default
  hostname TechPubAP7131
  floor 5thfloor
  layout-coordinates 1.0 2.0
  license AP aplicenseley@1234 aplicensekey@123
  rsa-key ssh rsa-key1
  location SanJose
  no contact
timezone Etc/UTC
  stats open-window 2 sample-interval 77 size 10
  country-code us
  sensor-server 1 ip 172.16.10.7
  channel-list 2.4GHz 1,2
  override-wlan test vlan-pool 8
  mac-name 00-04-96-4A-A7-08 5.8TestAP
  neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

- `no` Removes device’s configured timezone
7.2.19 trustpoint (device-config-mode)

Device Config Commands

Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server etc.

For more information on digital certificates and certificate authorities, see trustpoint (profile-config-mode).

NOTE: Certificates/trustpoints used in this command should be verifiable as existing on the device.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

trustpoint [cmp-auth-operator|https|radius-ca|radius-ca-ldaps|radius-server|radius-server-ldaps] <TRUSTPOINT-NAME>

Parameters
- trustpoint [cmp-auth-operator|https|radius-ca|radius-ca-ldaps|radius-server|radius-server-ldaps] <TRUSTPOINT-NAME>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustpoint</td>
<td>Assigns trustpoints to validate various services. The assigned trustpoint is used as the CA for validating the services.</td>
</tr>
<tr>
<td>cmp-auth-operator</td>
<td>Assigns an existing trustpoint to validate CMP auth operator. Once validated, CMP is used to obtain and manage digital certificates in a PKI network. Digital certificates link identity information with a public key enclosed within the certificate, and are issued by the CA. Use this command to specify the CMP-assigned trustpoint. When specified, devices send a certificate request to the CMP supported CA server, and download the certificate directly from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire. Note: When configured, this cmp-auth-operator trustpoint setting overrides the profile-level configuration.</td>
</tr>
<tr>
<td>https</td>
<td>Assigns an existing trustpoint to validate HTTPS</td>
</tr>
<tr>
<td>radius-ca</td>
<td>Assigns an existing trustpoint to validate client certificates in EAP</td>
</tr>
<tr>
<td>radius-ca-ldaps</td>
<td>Assigns an existing trustpoint to validate external LDAP server</td>
</tr>
<tr>
<td>radius-server</td>
<td>Assigns an existing trustpoint to validate RADIUS server certificate</td>
</tr>
<tr>
<td>radius-server-ldaps</td>
<td>Assigns an existing trustpoint to RADIUS server certificate to validate LDAP server</td>
</tr>
<tr>
<td>&lt;TRUSTPOINT-NAME&gt;</td>
<td>The following keyword is common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• &lt;TRUSTPOINT-NAME&gt; – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device). Note: By default, the system assigns the default-trustpoint to validate the following: https, radius-server, and radius-server-ldaps.</td>
</tr>
</tbody>
</table>
Examples
A device’s default HTTPS, RADIUS, and CMP certificate/trustpoint configuration is as follows:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include trustpoint
trustpoint https default-trustpoint
no trustpoint radius-ca
trustpoint radius-server default-trustpoint
no trustpoint radius-ca-ldaps
trustpoint radius-server-ldaps default-trustpoint
no trustpoint cmp-auth-operator
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#trustpoint https test
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include trustpoint
trustpoint https test
no trustpoint radius-ca
trustpoint radius-server default-trustpoint
no trustpoint radius-ca-ldaps
trustpoint radius-server-ldaps default-trustpoint
no trustpoint cmp-auth-operator
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```
7.2.20 mirror

Device Config Commands

Port mirroring enables forwarding of copies of incoming and/or outgoing packets from one or more ports in the switch to a specified destination port. The destination port serves as a duplicate image of the source ports and can be used to send packets to a network diagnostic tool without disrupting the behavior on the original port. Common diagnostic tools include network analyzers, remote monitoring probes, and IDS/IPS security devices. This feature facilitates network monitoring.

The NX4524 and NX6524 series service platforms support port mirroring. These devices mirror data packets transmitted or received on any of their GE ports (GE port 1 - 24). Both transmit and receive packets can be mirrored from a source to a destination port as needed to provide traditional spanning functionality on the 24 GE ports.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

mirror interface [INTERFACE-NAME|ge <1-24>] to interface [INTERFACE-NAME|ge <1-24>] {direction [any|inbound|outbound]}

Parameters


| mirror interface [INTERFACE-NAME|ge <1-24>] | Identifies the GE port used as the data source to span packets to the selected destination port. Use one of the following options to identify the source port: |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| • INTERFACE-NAME | Specifies the source port name |
| • ge <1-24> | Specifies the source GE port index |

Note: A source port cannot be a destination port.

Note: The source ports can be on the same or different VLANs.
### Usage Guidelines

All mirroring sessions must use the same destination port for packet capture.

### Examples

```plaintext
nx4524-470984(config-device-B6-22-D9-47-09-84)#mirror interface ge 3 to interface ge 24 direction any

nx4524-470984(config-device-B6-22-D9-47-09-84)#mirror interface ge 5 to interface ge 24 direction inbound

nx4524-470984(config-device-B6-22-D9-47-09-84)#mirror interface ge 7 to interface ge 24 direction outbound

nx4524-470984#show mirroring
```

<table>
<thead>
<tr>
<th>Session</th>
<th>Source</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ge3</td>
<td>ge24</td>
<td>any</td>
</tr>
<tr>
<td>2</td>
<td>ge7</td>
<td>ge24</td>
<td>inbound</td>
</tr>
<tr>
<td>3</td>
<td>ge5</td>
<td>ge24</td>
<td>outbound</td>
</tr>
</tbody>
</table>

(nx4524-470984#)

### Related Commands

| no | Disables data packets mirroring on GE ports |
7.2.21 raid

Device Config Commands

Enables chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on a service platform.

The NX9000 (NX9000, NX9500 and NX9510) series service platforms include a single Intel MegaRAID controller (virtual drive) with RAID-1 mirroring support enabled. The online virtual drive supports up to two physical drives that could require hot spare substitution if a drive were to fail. The WiNG software allows you to manage the RAID controller event alarm and syslogs supporting the array hardware from the service platform user interface without rebooting the service platform BIOS.

Although RAID controller drive arrays are available only on the NX9000 series service platforms, they can be administrated on behalf of a NX9000 profile by a different model service platform or wireless controller.

For more information on RAID, see raid.

Supported in the following platforms:

- Service Platforms — NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

raid alarm enable

Parameters

- raid alarm enable

| alarm enable | Enables audible alarm, which is triggered a RAID drives fails. When triggered the alarm can be disabled by executing the raid > silence command in the device's Priv Exec mode. |

Examples

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#raid alarm enable

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context

nx9000 B4-C7-99-6C-88-09
use profile default-nx9000
use rf-domain default
hostname nx9500-6C8809
ip default-gateway 192.168.13.2
interface gel
switchport mode access
switchport access vlan 1
interface vlan1
ip address 192.168.13.13/24
logging on
logging console warnings
logging buffered warnings
raid alarm enable
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#

Related Commands

- no — Disables RAID alarm
7.3 T5 Profile Config Commands

PROFILES

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE’s physical wallplate connection and phone jack.

To navigate to this instance, use the following commands:

<DEVICE>(config-profile-<PROFILE-NAME>)#?

T5 Profile Mode commands:

- **cpe** T5 CPE configuration
- **interface** Select an interface to configure
- **ip** Internet Protocol (IP)
- **no** Negate a command or set its defaults
- **ntp** Configure NTP
- **override-wlan** Configure RF Domain level overrides for wlan
- **t5** T5 configuration
- **t5-logging** Modify message logging facilities
- **use** Set setting to use
- **clrscr** Clears the display screen
- **commit** Commit all changes made in this session
- **do** Run commands from Exec mode
- **end** End current mode and change to EXEC mode
- **exit** End current mode and down to previous mode
- **help** Description of the interactive help system
- **revert** Revert changes
- **service** Service Commands
- **show** Show running system information
- **write** Write running configuration to memory or terminal

<DEVICE>(config-profile-<PROFILE-NAME>)#

The following table summarizes T5 profile configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cpe</strong></td>
<td>Configures T5 CPE related settings (IP address range and VLAN)</td>
<td>page 7-476</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>Configures the T5 controller’s interfaces</td>
<td>page 7-477</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Configures the default gateway’s IP address</td>
<td>page 7-479</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Removes or reverts this T5 controller profile settings</td>
<td>page 7-480</td>
</tr>
<tr>
<td><strong>ntp</strong></td>
<td>Configures the NTP server associated with this T5 profile</td>
<td>page 7-481</td>
</tr>
<tr>
<td><strong>override-wlan</strong></td>
<td>Configures the RF Domain level overrides for applied on a WLAN on this T5 profile</td>
<td>page 7-482</td>
</tr>
<tr>
<td><strong>t5</strong></td>
<td>Configures the logged T5 controller’s country of operation</td>
<td>page 7-483</td>
</tr>
<tr>
<td><strong>t5-logging</strong></td>
<td>Configures a maximum of 5 (five) remote hosts capable of receiving syslog messages from this selected T5 controller</td>
<td>page 7-484</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>Defines this T5 profile’s management settings</td>
<td>page 7-485</td>
</tr>
</tbody>
</table>
7.3.1 **cpe**

- **T5 Profile Config Commands**

Configures T5 CPE related settings

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

cpe address vlan <1-4094> <START-IP> <END-IP>

**Parameters**

- cpe address vlan <1-4094> <START-IP> <END-IP>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;START-IP&gt; &lt;END-IP&gt;</td>
<td>Configures the range of IP addresses that can be assigned to the CPEs managed by this T5 controller</td>
</tr>
<tr>
<td>• &lt;START-IP&gt;</td>
<td>Specify the first IP address in the range.</td>
</tr>
<tr>
<td>• &lt;END-IP&gt;</td>
<td>Specify the last IP address in the range.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile-T5TestProfile)#cpe address vlan 200 192.168.13.26 192.168.13.30

nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
  no autoinstall configuration
  no autoinstall firmware
  interface vlan1
  interface vlan4090
  interface fe 5 2
  ..............................................................
  interface radio 11 1
  interface fe 9 2
  interface radio 18 1
  interface fe 9 1
  use firewall-policy default
  service pm sys-restart

  cpe address vlan 200 192.168.13.26 192.168.13.30

nx9500-6C8809(config-profile-T5TestProfile)#
```
7.3.2 interface

T5 Profile Config Commands

Configures the T5 controller’s interfaces

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

Syntax

interface [<WORD>|dsl|fe|ge|radio|vlan]

Parameters

- interface [<WORD>|dsl|fe|ge|radio|vlan]

<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Configures the interface identified by the &lt;WORD&gt; keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsl &lt;1-24&gt;</td>
<td>Configures the specified DSL interface. A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating used by controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5’s management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use DSL as their high speed Internet access mechanism using the CPE’s physical wallplate connection and phone jack.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-24&gt; – Specify the DSL port index from 1 - 24.</td>
</tr>
<tr>
<td>fe &lt;1-24&gt; &lt;1-2&gt;</td>
<td>Configures the specified FastEthernet interface. The T5 controller has the following FastEthernet port designations: fe1-fe2 (fe1-fe2 are for up to 24 CPE devices managed by a T5 controller).</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-24&gt; – Specify the DSL port index from 1 - 24.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-2&gt; – Specify the FastEthernet interface to configure.</td>
</tr>
<tr>
<td></td>
<td>Note: In the FastEthernet interface configuration mode, specify the interface settings.</td>
</tr>
<tr>
<td>ge &lt;1-2&gt;</td>
<td>Configures the specified GigabitEthernet interface. The GE ports can be RJ-45 or fiber ports supporting 10/100/1000Mbps.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-2&gt; – Specify the interface index from 1 - 2.</td>
</tr>
<tr>
<td></td>
<td>Note: In the GigabitEthernet interface configuration mode, specify the interface settings.</td>
</tr>
<tr>
<td>radio &lt;1-24&gt;</td>
<td>Configures the specified radio interface. T5 controller managed CPE device radios can have their radio configurations overridden once their radios have successfully associated and have been provisioned by the adopting controller, service platform, or peer model AP controller access point.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-2&gt; – Specify the radio interface index from 1 - 24.</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Configures the specified VLAN interface. Once configured, the VLAN interface provides layer 3 (IP) T5 controller access or provides layer 3 service on a VLAN. The VLAN interface defines which IP address is associated with each VLAN ID a T5 controller is connected to. A VLAN interface is created for the default VLAN (VLAN 1) to enable remote administration. This interface is also used to map VLANs to IP4 and IPv6 formatted IP address ranges. This mapping determines the destination for routing.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the VLAN interface index from 1 - 4094.</td>
</tr>
<tr>
<td></td>
<td>Note: In the VLAN configuration mode, specify the interface’s primary IP address in the A.B.C.D/M format. Optionally specify the secondary IP address.</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-profile-t5Profile)#interface dsl 1

rfs7000-37FABE(config-profile-t5Profile-if-dsl1)#?

Interface configuration commands:

- **description** Port description
- **ds-interleaver** Enable impulse noise protection in the downstream direction
- **ds-max-datarate** Configure maximum allowed downstream rate for the interface
- **ds-min-margin** Configure the minimum downstream signal-to-noise (SNR) ratio margin
- **ds-target-margin** Configure the desired downstream signal-to-noise (SNR) ratio margin
- **duplex** Set duplex to interface
- **flowcontrol** Set flowcontrol to interface
- **line-power** Use the line-power command to apply power to the interface
- **no** Negate a command or set its defaults
- **qos** QOS settings
- **shutdown** Shutdown the selected interface
- **speed** Configure speed
- **switchport** Set switching mode characteristics
- **us-interleaver** Enable impulse noise protection in the upstream direction
- **us-max-datarate** Configure maximum allowed upstream rate for the interface
- **us-min-margin** Configure the minimum upstream signal-to-noise (SNR) ratio margin
- **us-target-margin** Configure the desired upstream signal-to-noise (SNR) ratio margin

**clrscr** Clears the display screen
**commit** Commit all changes made in this session
**do** Run commands from Exec mode
**end** End current mode and change to EXEC mode
**exit** End current mode and down to previous mode
**help** Description of the interactive help system
**revert** Revert changes
**service** Service Commands

--More--

rfs7000-37FABE(config-profile-t5Profile-if-dsl1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the selected interface configuration on the T5 device</td>
</tr>
</tbody>
</table>
### 7.3.3 ip

#### T5 Profile Config Commands

Configures the default gateway’s IP address

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

#### Syntax

```
ip default-gateway <IP>
```

#### Parameters

- `ip default-gateway <IP>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip default-gateway</td>
<td>Enter the default gateway’s IP address in the A.B.C.D format.</td>
</tr>
</tbody>
</table>

#### Examples

```
nx9500-6C8809(config-profile-t5Profile)#ip default-gateway 192.168.13.7

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
ip default-gateway 192.168.13.7
no autoinstall configuration
no autoinstall firmware
interface vlan1
interface vlan4090
interface fe 5 2
interface ge 2
interface ge 1
interface fe 5 1
--More--
nx9500-6C8809(config-profile-t5Profile)#
```
### T5 Profile Config Commands

Removes or reverts this T5 controller profile settings

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

#### Syntax

```no [interface|ntp|override-wlan|t5-logging|use]```

- `no interface vlan <2-4094>`
- `no ntp server <IP>`
- `no override-wlan <WLAN-NAME> vlan`
- `no t5-logging host <IP>`
- `no use management-policy`

#### Parameters

- `no <PARAMETERS>`

### Examples

```bash
nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
  ip default-gateway 192.168.13.7
  no autoinstall configuration
  no autoinstall firmware
  interface vlan1
  interface vlan4090
  ..........................................................
  use firewall-policy default
  ntp server 192.168.13.2
  service pm sys-restart

nx9500-6C8809(config-profile-t5Profile)#no ntp server 192.168.13.2

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
  ip default-gateway 192.168.13.7
  no autoinstall configuration
  no autoinstall firmware
  interface vlan1
  interface vlan4090
  ..........................................................
  use firewall-policy default
  service pm sys-restart
```

`no <PARAMETERS>` Removes or reverts to default the selected T5 profile’s or device’s settings
7.3.5 ntp

**T5 Profile Config Commands**

Configures the NTP server associated with this T5 profile. T5 controllers, using this profile, will obtain their system time from the specified NTP server resources.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
ntp server <IP>
```

**Parameters**

- `ntp server <IP>`

**Examples**

```
nx9500-6C8809(config-profile-t5Profile)#ntp server 192.168.13.2
```

```
nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface dsl 5
 ....................................................
 use firewall-policy default
 ntp server 192.168.13.2
 service pm sys-restart
 nx9500-6C8809(config-profile-t5Profile)#
```

**Related Commands**

```
no
```

Removes the NTP server’s IP address
7.3.6 **override-wlan**

**T5 Profile Config Commands**

Use this option to configure RF Domain level configuration for WLAN. The override configured here are applied to all T5 devices using this T5 profile.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
override-wlan <WLAN-NAME> vlan <1-4094>
```

**Parameters**

- `override-wlan <WLAN-NAME> vlan <1-4094>`

<table>
<thead>
<tr>
<th>override-wlan &lt;WLAN-NAME&gt;</th>
<th>Overrides the specified WLAN's VLAN configuration &lt;WLAN-NAME&gt; – Specify the WLAN's name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Specify the new VLAN option &lt;1-4094&gt; – Specify the VLAN from 1 - 4094.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the WLAN SJOffWLan configuration:

```
nx9500-6C8809(config-wlan-SJOffWLan)#show context
wlan SJOffWLan
  description "SJ Office WLAN"
  ssid SJOffWLan
  vlan 468
  bridging-mode local
  encryption-type ccmp
  authentication-type eap-psk
  use aaa-policy test
```

The following example overrides the SJOffWLan WLAN's VLAN configuration on the T5 profile:

```
nx9500-6C8809(config-profile-testT5)#override-wlan SJOffWLan vlan 30
```

```
nx9500-6C8809(config-profile-testT5)#show context include-factory | include override-wlan
  override-wlan SJOffWLan vlan 30
```

**Related Commands**

| no | Removes the RF Domain level overrides for applied on a WLAN on this T5 profile |
7.3.7 t5

**T5 Profile Config Commands**

Configures this T5 controller's country of operation

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

t5 country-code <WORD>

**Parameters**

- t5 country-code <WORD>

<table>
<thead>
<tr>
<th>country-code &lt;WORD&gt;</th>
<th>Configures the 2 letter ISO-3166 country code for this T5 controller</th>
</tr>
</thead>
</table>

**Examples**

nx9500-6C8809(config-profile-T5TestProfile)#t5 country-code us

nx9500-6C8809(config-profile-T5TestProfile)#show context profile t5 T5TestProfile
no autoinstall configuration
no autoinstall firmware
interface vlan1
interface vlan4090
interface fe 5 2

interface fe 9 1
use firewall-policy default
service pm sys-restart
t5 country-code US
cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
7.3.8 t5-logging

**T5 Profile Config Commands**

Configures a maximum of 5 (five) remote hosts capable of receiving syslog messages from this selected T5 controller

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
t5-logging host <IP> severity [error|info|notice|trace|warning] facility [local0|local1|local2|local3|local4|local5|local6|local7]
```

**Parameters**

- `t5-logging host <IP> severity [error|info|notice|trace|warning] facility [local0|local1|local2|local3|local4|local5|local6|local7]`

<table>
<thead>
<tr>
<th>t5-logging host &lt;IP&gt;</th>
<th>Configures syslog message logging settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;IP&gt;</td>
<td>- Configures the external syslog remote host resource's IP address. This is the host dedicated to receive T5 syslog messages.</td>
</tr>
</tbody>
</table>

| severity [error|info|notice|trace|warning] | Configures the syslog message filtering severity level. The options are: |
|-------------------------------------------------|-------------------------------------------------------------------|
| - Error – Only forwards error and above syslog event messages. |
| - Info – Only forwards informational and above syslog event messages. |
| - notice – Only forwards syslog notices relating to general device operational events. These are events that are of more interest than the “info” events.  |
| - trace – Only forwards trace routing event messages  |
| - warning – Only forwards warnings and above syslog event messages |

| facility [local0|local1|local2|local3|local4|local5|local6|local7] | Configures the facility level for log messages sent to the syslog server. The facility level specifies the type of program logging the message. Specifying the facility level allows the configuration file to specify that message handling will vary with varying facility type. The options are: local0, local1, local2, local3, local4, local5, local6, local7. The default value is local7. |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------|

**Examples**

```
nx9500-6C8809(config-profile-T5TestProfile)#t5-logging host 192.168.13.10 severity warning facility local6
```

```
nx9500-6C8809(config-profile-T5TestProfile)#show context profile t5 T5TestProfile
    t5-logging host 192.168.13.10 severity warning facility local6
    no autoinstall configuration
    no autoinstall firmware
    t5 country-code US
cpe address vlan 200 192.168.13.26 192.168.13.30
```

**Related Commands**

- `no` | Modifies message logging severity level and facilities
7.3.9 use

T5 Profile Config Commands

Associates a management policy with this T5 profile. The specified policy is applied to all T5 controllers using this profile.

Supported in the following platforms:

• Wireless Controllers — RFS4000, RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

Syntax

use management-policy <POLICY-NAME>

Parameters

• use management-policy <POLICY-NAME>

Examples

nx9500-6C8809(config-profile-t5Profile)#use management-policy default
Trustpoints HTTPS Server and RSA keys for SSH can be configured with 'trustpoint' and 'rsa-key' commands in device context
nx9500-6C8809(config-profile-t5Profile)#

Related Commands

no

Removes the management policy used with this T5 profile
7.4 EX3524 & EX3548 Profile/Device Config Commands

PROFILES

Creates a new EX3524 and EX3548 profile and enters its configuration mode.

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#profile ex35xx <EX35XX-PROFILE-NAME>
```

Where ex35xx can be a EX3524 or a EX3548 device type.

```
<DEVICE>(config-profile-<EX35XX-PROFILE-NAME>)#?
```

EX35XX Profile Mode commands:

- `interface` Select an interface to configure
- `ip` Internet Protocol (IP)
- `no` Negate a command or set its defaults
- `power` EX3500 Power over Ethernet Command
- `upgrade` Configures upgrade option for ex3500 system
- `use` Set setting to use
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

The following table summarizes EX3524 and EX3548 profile/device configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Selects an interface type and enters the selected interface’s configuration mode</td>
<td>page 7-487</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Configures the default gateway through which this EX35XX switch can reach other subnets</td>
<td>page 7-507</td>
</tr>
<tr>
<td><code>power</code></td>
<td>Enables power inline compatibility mode on this EX35XX profile</td>
<td>page 7-508</td>
</tr>
<tr>
<td><code>upgrade</code></td>
<td>Configures adopted EX35XX switch upgrade settings</td>
<td>page 7-509</td>
</tr>
<tr>
<td><code>use</code></td>
<td>Applies an EX3500 management policy to this EX35XX profile</td>
<td>page 7-510</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Removes or reverts this EX35XX profile’s settings</td>
<td>page 7-511</td>
</tr>
</tbody>
</table>
### 7.4.1 interface

**EX3524 & EX3548 Profile/Device Config Commands**

This command selects an interface type and enters the selected interface’s configuration mode. The EX35XX switch has GE and VLAN interfaces. Select the interface type and provide the interface ID to enter its configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Selects an interface type and enters the selected interface’s configuration mode</td>
<td>page 7-488</td>
</tr>
<tr>
<td>interface-ge-config</td>
<td>Summarizes GE interface configuration mode commands</td>
<td>page 7-490</td>
</tr>
<tr>
<td>commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface-vlan-config</td>
<td>Summarizes VLAN interface configuration mode commands</td>
<td>page 7-503</td>
</tr>
</tbody>
</table>
7.4.1.1 interface

Selects the EX35XX interface type and enters the selected interface’s configuration mode.

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
interface [ge 1 <1-48>|vlan <1-4094>]
```

Parameters
- interface [ge 1 <1-48>|vlan <1-4094>]

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| ge 1 <1-48>| Selects a GE interface to configure  
|  1 – Configures the GE interface unit identifier as 1  
|  <1-48> – Configures the physical port number from 1 - 24/48  
|  **Note**: For the EX3524 model switch the GE port range is 1-24, and for the EX3548 it is 1-48. |
| vlan <1-4094>| Selects a VLAN interface to configure  
|  <1-4094> – Specify the VLAN interface ID from 1 - 4094. |

Examples
```
nx4500-5CFA8E(config-profile-testEX35XX)#interface vlan 1
nx4500-5CFA8E(config-profile-testEX35XX-if-vlan1)#?
commands:
ip  Internet Protocol (IP)
no  Negate a command or set its defaults
clrscr  Clears the display screen
commit  Commit all changes made in this session
do  Run commands from Exec mode
dc  End current mode and change to EXEC mode
exit  End current mode and down to previous mode
help  Description of the interactive help system
revert  Revert changes
service  Service Commands
show  Show running system information
write  Write running configuration to memory or terminal
```
```
nx4500-5CFA8E(config-profile-testEX35XX-if-vlan1)#
```
```
nx4500-5CFA8E(config-profile-testEX35XX)#interface ge 1 1
nx4500-5CFA8E(config-profile-testEX35XX-if-ge1-1)#?
commands:
access-group  Access group to bind a port to an ACL name
no  Negate a command or set its defaults
port  Configures the characteristics of the port
power  EX3500 Power over Ethernet Command
shutdown  Shutdown the selected interface
speed-duplex  Configures speed and duplex operation
switchport  Configures switch mode characteristics
use  Set setting to use
clrscr  Clears the display screen
commit  Commit all changes made in this session
do            Run commands from Exec mode
end           End current mode and change to EXEC mode
exit          End current mode and down to previous mode
help          Description of the interactive help system
revert        Revert changes
service       Service Commands
show          Show running system information
write         Write running configuration to memory or terminal

nx4500-5CFA8E(config-profile-testEX35XX-if-ge1-1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes this interface (GE/VLAN) settings from the EX35XX profile or device</td>
</tr>
<tr>
<td>interface-ge-config commands</td>
<td>Summarizes GE interface configuration mode commands</td>
</tr>
<tr>
<td>interface-vlan-config commands</td>
<td>Summarizes VLAN interface configuration mode commands</td>
</tr>
</tbody>
</table>
7.4.1.2 interface-ge-config commands

The following table lists the EX35XX GE interface configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group</td>
<td>Binds an EX3500 ACL to the selected port</td>
<td>page 7-491</td>
</tr>
<tr>
<td>port</td>
<td>Enables port monitoring on the selected port</td>
<td>page 7-492</td>
</tr>
<tr>
<td>power</td>
<td>Turns power on or off for the selected port</td>
<td>page 7-494</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the selected port</td>
<td>page 7-496</td>
</tr>
<tr>
<td>speed-duplex</td>
<td>Configures the speed and duplex mode of the selected port when auto-negotiation is disabled. Auto-negotiation is enabled by default.</td>
<td>page 7-497</td>
</tr>
<tr>
<td>switch-port</td>
<td>Configures the switch mode characteristics of the selected port</td>
<td>page 7-498</td>
</tr>
<tr>
<td>use</td>
<td>Applies a EX3500 QoS policy map with the selected port</td>
<td>page 7-500</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the selected port's settings</td>
<td>page 7-501</td>
</tr>
</tbody>
</table>
### 7.4.1.2.1 access-group

**interface-ge-config commands**

Binds an EX3500 ACL to the selected port

When applied to the port, the ACL takes effect. Only one ACL can be bound to a port at a time. In case you bind a new ACL to a port with an existing ACL binding, the old binding is replaced with the new one.

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```plaintext
access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME> in {time-range <TIME-RANGE-NAME>}
```

**Parameters**

- **access-group** [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME> in {time-range <TIME-RANGE-NAME>}

<table>
<thead>
<tr>
<th>access-group</th>
<th>Binds a EX3500 ACL with this GE port. Select ACL type and specify the ACL name. The ACL should be existing and configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex3500-ext-access-list &lt;ACL-NAME&gt;</td>
<td>Binds an existing and configured EX3500 extended ACL</td>
</tr>
<tr>
<td>ex3500-std-access-list &lt;ACL-NAME&gt;</td>
<td>Binds an existing and configured EX3500 standard ACL</td>
</tr>
<tr>
<td>mac-access-list &lt;ACL-NAME&gt;</td>
<td>Binds an existing and configured EX3500 MAC ACL</td>
</tr>
<tr>
<td>in</td>
<td>Applies the specified ACL to all incoming packets</td>
</tr>
<tr>
<td>time-range &lt;TIME-RANGE-NAME&gt;</td>
<td>Optional. Associates a EX3500 absolute or periodic time range with this access group. The specified ACL is bound to the port during the time period specified by the associated time range.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context interface ge 1 20
   access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

**Related Commands**

- **no** Removes the GE port EX3500 ACL binding
7.4.1.2.2 port

*interface-ge-config commands*

Enables port monitoring on the selected port. This allows the port to monitor specified ports and/or MAC address(es). When enabled, the switch sends a copy of the network packets seen on the specified switch port (or VLAN interface) to the monitoring switch port. These packets are analyzed and debugged to provide vital information, such as network performance, intrusion alerts etc.

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| port monitor ethernet 1 <1-52> {both|rx|tx} | Configures the characteristics of this GE port
  - monitor – Enables monitoring of another port
  - ethernet 1 – Selects Ethernet interface and configures the port identifier as 1
  - <1-52> – Configures the Ethernet unit number from 1 - 52 |
| port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME> | After specifying the port, optionally configure the following:
  - both – Optional. Monitors both incoming and outgoing traffic
  - rx – Optional. Monitors only incoming traffic
  - tx – Optional. Monitors only outgoing traffic |
| port monitor mac-address <MAC> | Configures the characteristics of this GE port
  - monitor – Enables monitoring of another port |
| port monitor vlan <1-4094> | Configures the characteristics of this GE port
  - monitor – Enables monitoring of another port |

**Supported in the following platforms:**
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Parameters**
- port monitor ethernet 1 <1-52> {both|rx|tx}
port monitor mac-address <MAC>

Configures the characteristics of this GE port
- monitor – Enables monitoring of another port

mac-address <MAC>

Configures the MAC address to monitor
- <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.

port monitor vlan <1-4094>

Configures the VLAN interface to monitor
- <1-4094> – Specify the VLAN ID from 1 - 4094.

Examples

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
  port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

Related Commands

no

Disables port monitoring on the selected port and removes the settings
7.4.1.2.3 power

interface-ge-config commands

Enables power allocation to the selected port. When enabled, the power is allocated to this port. Use the command to configure the power allocation settings, such as maximum power allocated, priority level of this port in connection with power allocation, and the time range within which these power settings are applied.

This option is enabled by default.

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
power inline {maximum|priority|time-range}
power inline {maximum allocation milliwatts <3000-34200>}
power inline {priority [critical|high|low]}
power inline {time-range <TIME-RANGE-NAME>}
```

Parameters

- **power inline {maximum allocation milliwatts <3000-34200>}**
  - Optional. Configures the maximum power allocation, in milliwatts, for this port
  - `<3000-34200>` – Specify a value from 3000 - 34200 milliwatts. The default is 34200 milliwatts.

- **power inline {priority [critical|high|low]}**
  - Optional. Configures the PoE power priority as:
    - **critical** – Configures the PoE power priority as critical
    - **high** – Configures the PoE power priority as high
    - **low** - Configures the PoE power priority as low (this is the default setting)

- **power inline {time-range <TIME-RANGE-NAME>}**
  - Optional. Binds an EX3500 time range to this port
  - `<TIME-RANGE-NAME>` – Specify the time range name (should be existing and configured).

Examples

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline maximum allocation milliwatts 30000

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline priority critical

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline time-range EX3500_TimeRange_01
```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
  interface ge 1 20
    power inline maximum allocation milliwatts 30000
    power inline priority critical
    power inline time-range EX3500_TimeRange_01
    access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
    port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables power allocation to the selected port</td>
</tr>
</tbody>
</table>
7.4.1.2.4 shutdown

interface-ge-config commands
Shuts down the selected port

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax
shutdown

Parameters
None

Examples
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#shutdown

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
  shutdown
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
  port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

Related Commands

| no | Brings up a shutdown port |
7.4.1.2.5 speed-duplex

*interface-ge-config commands*

Configures the speed and duplex mode of the selected port when auto-negotiation is disabled. Auto-negotiation is enabled by default.

This option is disabled by default.

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
speed-duplex [100full|100half|10full|10half]
```

**Parameters**

- `speed-duplex [100full|100half|10full|10half]`

**Examples**

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#speed-duplex 100half
```

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
  interface ge 1 20
     shutdown
     speed-duplex 100half
     power inline maximum allocation milliwatts 30000
     power inline priority critical
     power inline time-range EX3500_TimeRange_01
     access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
     port monitor vlan 20
```

**Related Commands**

```
no
```

Removes the speed and duplex settings configured for this EX35XX profile.
7.4.1.2.6 switch-port

▪ interface-ge-config commands

Configures the switch mode characteristics of the selected port

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

switchport [allowed|l2protocol-tunnel|mode|native]

switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>]

switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]

switchport mode [access|hybrid|trunk]

switchport native

Parameters

- switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>]

| switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>] | Configures VLAN groups on the selected interface. |
|------------------------------------------------------------|-------------------------------------------------|
| - add <VLAN-ID> – Configures the list of VLAN identifiers to add. When the add option is used, the interface is assigned to the specified VLANs, and membership in all previous VLANs is retained. |
| - <VLAN-ID> – Specify the list of VLANs to add. |
| - none – Removes all VLANs from the current list |
| - remove <VLAN-ID> – Configures the list of VLAN identifiers to remove. When the remove option is used, the specified VLANs are removed from the current list. |
| - <VLAN-ID> – Specify the list of VLANs to remove. |

- switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]

| switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp] | Enables layer 2 protocol tunneling (L2PT) for the specified protocol. Specify the protocol: |
|--------------------------------------------------------|----------------------------------------------------------------------------------|
| - cdp – Cisco Discovery Protocol | - lldp – Link Layer Discovery Protocol |
| - pvst+ – Cisco Per VLAN Spanning Tree Plus | - spanning-tree – Spanning Tree (STP, RSTP, MSTP) |
| - vtp – Cisco VLAN Trunking Protocol | L2PT is disabled for all of the above specified protocols by default. |
### switchport mode [access|hybrid|trunk]

- **switchport mode [access|hybrid|trunk]**

  Configures the VLAN membership mode for this port
  - **access** – The port is configured as an access VLAN interface. It transmits and receives packets untagged frames on a single VLAN.

  **Contd..**
  - **trunk** – Configures the selected port as an end-point for a VLAN trunk. A trunk link is configured between two switches, and it carries frames on more than one VLANs. These frames are tagged in order to identify the source VLAN. Frames belonging to the port’s default VLAN are also transmitted as tagged frames.
  - **hybrid** – Configures the selected port as a hybrid VLAN interface. When configured as hybrid, the port can transmit either tagged or untagged frames. This is the default setting.

### switchport native vlan <1-4094>

- **switchport native vlan <1-4094> in**

  Configures the VLAN membership mode for this port
  - **native vlan <1-4094>** – Configures the port’s VLAN ID (PVID) (this is the port’s default VLAN ID). Frames from the specified VLAN ingress untagged at this port. The default value is 1.

  When using **access** mode, and an interface is assigned to a new VLAN, the port’s VLAN ID (PVID) is automatically set to the identifier for that VLAN. When using **hybrid** mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.

### Examples

```plaintext
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#switchport mode access

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
    shutdown
    speed-duplex 100half
switchport mode access
    power inline maximum allocation milliwatts 30000
    power inline priority critical
    power inline time-range EX3500_TimeRange_01
    access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
    port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

### Related Commands

| **no**       | Removes the selected port’s switchport characteristics |
7.4.1.2.7 use

Appplies a EX3500 QoS policy map with the selected port

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in

Parameters

- use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in | Applies a EX3500 QoS policy map with the selected port
  - <EX3500-QoS-POLICY-MAP-NAME> – Specify the EX3500 QoS policy map name (should be existing and configured)
  - in – Applies the specified policy to traffic ingressing at the selected port. |

Examples

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#use ex3500-policy-map in test

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
  shutdown
  speed-duplex 100half
  switchport mode access
  use ex3500-policy-map in test
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
  port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

Related Commands

no | Disassociates the EX3500 QoS policy map linked to this EX3500 profile
7-500 WiNG 5.8.1 CLI Reference Guide

7.4.1.2.8 no

interface-ge-config commands

Removes or reverts the selected port's settings

Supported in the following platforms:

- Switches — EX3524, EX3548

Syntax

```
no [access-group|port|power|shutdown|speed-duplex|switchport|use]
no access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME> in

no port monitor [ethernet|ex3500-ext-access-list|ex3500-std-access-list|mac-access-list|mac-address|vlan]
no port monitor ethernet 1 <1-52>
no port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME>
no port monitor mac-address <MAC>
no port monitor vlan <1-4094>
no power inline {maximum allocation|priority|time-range}
no shutdown
no speed-duplex
no switchport [l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]|native vlan]
no use ex3500-policy-map in
```

Parameters

- no <PARAMETERS>

no <PARAMETERS> Removes or reverts the selected port's settings based on the parameters passed

Examples

The following example shows the EX3524 profile's GE port 20's settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
  shutdown
  speed-duplex 100half
  switchport mode access
  use ex3500-policy-map in test
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no shutdown
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no power inline maximum allocation
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no use ex3500-policy-map in
```

```
The following example shows the EX3524 profile's GE port 20's settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
  interface ge 1 20
    speed-duplex 100half
    switchport mode access
    power inline maximum allocation milliwatts 32400
    power inline priority critical
    power inline time-range EX3500_TimeRange_01
    access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
    port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```
7.4.1.3 interface-vlan-config commands

The following table lists the VLAN interface configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Configures IP related settings for this VLAN interface</td>
<td>page 7-504</td>
</tr>
<tr>
<td>no</td>
<td>Removes the IP related settings configured for this VLAN interface</td>
<td>page 7-506</td>
</tr>
</tbody>
</table>
7.4.1.3.1  ip

`interface-vlan-config commands`

Configures IP related settings for this VLAN interface

Supported in the following platforms:

- **Switches** — EX3524, EX3548
- **Wireless Controllers** – RFS4000, RFS6000, RFS7000
- **Service Platforms** – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
ip address [<IP/M]|bootp|dhcp]
ip address <IP/M> {default-gateway <IP>|secondary <IP>}
ip address [bootp|dhcp]
```

**Parameters**

- **ip address <IP/M> {default-gateway <IP>|secondary <IP>}**

  Manually configures the selected VLAN interface’s primary and secondary IPv4 addresses. It also allows to optionally configure the default gateway.
  - **<IP/M>** – Manually configures this VLAN interface’s IP address in the A.B.C.D/M format. Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask can be either in the traditional format xxx.xxx.xxx.xxx or use classless format with the range /5 to /32. For example the subnet 255.255.224.0 would be /19.
  - **default-gateway <IP>** – Optional. Configures the default gateway’s IP address. This is the gateway through which this switch can reach other subnets not found in the local routing table. Before specifying the default gateway, ensure that the network interface directly connecting to the gateway is configured on the route. By default no gateway is specified.
  - **secondary <IP>** – Optional. Configures this VLAN interface’s secondary IP address

- **ip address [bootp|dhcp]**

  Enables a DHCP or Bootp server to provide the primary IPv4 address for the selected VLAN interface
  - **bootp** – Enables the VLAN interface to get its IP address from a Bootp server
  - **dhcp** – Enables the VLAN interface to get its IP address from a DHCP server

  If selecting DHCP/Bootp, ensure that a server on the network has been configured to provide the necessary configuration to the switch. Using DHCP or Bootp results in frequent connectivity loss between the browser interface and the switch. Further, DHCP and Bootp cannot configure secondary IP addresses needed for multinetting.
Examples

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#ip address 192.168.13.28/24 default-gateway 192.168.13.13

nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context interface vlan 20
    ip address 192.168.13.28/24 default-gateway 192.168.13.13
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the IP address configured for this VLAN interface</td>
</tr>
</tbody>
</table>
7.4.1.3.2 no

`interface-vlan-config commands`

Removes the IP related settings configured for this VLAN interface

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
no ip address [<IP/M>|bootp|dhcp]
```

**Parameters**
- `no <PARAMETERS>`

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes this EX3500’s selected VLAN’s settings based on the parameters passed</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the interface VLAN 20 setting before the ‘no’ command is executed:

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
  interface vlan 20  
    ip address 192.168.13.28/24 default-gateway 192.168.13.13
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#no ip address 192.168.13.28/24
```

The following example shows the interface VLAN 20 setting after the ‘no’ command is executed:

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
  interface vlan 20
```

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```
7.4.2 ip

EX3524 & EX3548 Profile/Device Config Commands

Configures the default gateway through which this EX35XX switch can reach other subnets

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
ip default-gateway <IP>
```

Parameters

- `ip default-gateway <IP>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip default-gateway &lt;IP&gt;</strong></td>
<td>Configures the default gateway's IP address in the A.B.C.D format</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP&gt;</code> – Specify the IP address.</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809(config-profile-testEX3524)#ip default-gateway 192.168.13.13

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
  ip default-gateway 192.168.13.13
  no autoinstall configuration
  no autoinstall firmware
  interface ge 1 17
  interface ge 1 16
  interface ge 1 15
  interface ge 1 14
  interface ge 1 13
  interface ge 1 12
  interface ge 1 11
  --More--
  interface ge 1 21
  use firewall-policy default
  service pm sys-restart
```

```
nx9500-6C8809(config-profile-testEX3524)#
```
### 7.4.3 power

**EX3524 & EX3548 Profile/Device Config Commands**

Enables power inline compatibility mode on this EX35XX profile. This option is disabled by default.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```plaintext
power inline compatible
```

**Parameters**

- `power inline compatible`

**Examples**

```plaintext
nx9500-6C8809(config-profile-testEX3524)#power inline compatible

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
  ip default-gateway 192.168.13.13
  power inline compatible
  no autoinstall configuration
  no autoinstall firmware
  interface ge 1 17
  interface ge 1 16
  interface ge 1 15
  interface ge 1 14
  interface ge 1 13
  interface ge 1 12
  --More--

nx9500-6C8809(config-profile-testEX3524)#
```
EX3524 & EX3548 Profile/Device Config Commands

Configures adopted EX35XX switch upgrade settings

For an EX35XX switch to adopt to and be managed by a WiNG controller, you need to upload two images on the switch. An operation code (opcode) image and an adopted image. The opcode image functions as an operating system that enables the WiNG controller to communicate with the EX35XX switch. This command allows you to configure the EX35XX's opcode image upgrade settings.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

upgrade opcode [auto|path <LINE>|reload]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrade opcode</td>
<td>Configures the opcode image upgrade settings</td>
</tr>
<tr>
<td>auto</td>
<td>Enables automatic upgrade</td>
</tr>
<tr>
<td>path &lt;LINE&gt;</td>
<td>Configures the location of the opcode image</td>
</tr>
<tr>
<td>reload</td>
<td>Enables automatic reload after successful loading of the opcode image</td>
</tr>
</tbody>
</table>

Examples

```
<EX35XX-DEVICE>#show version
Unit 1
Serial Number          : 14136520900352
Hardware Version       : R01
EPLD Version           : 0.00
Number of Ports        : 28
Main Power Status      : Up
Role                   : Master
Loader Version         : 5.0.0.1-01A
Linux Kernel Version   : 2.6.22.18
Boot ROM Version       : 0.0.0.1
Operation Code Version : 5.0.0.0-03D
Adopted Version        : 5.8.1.0-028D
<EX35XX-DEVICE>#

nx9500-6C8809(config-profile-testEX3524)#upgrade auto
nx9500-6C8809(config-profile-testEX3524)#upgrade reload
nx9500-6C8809(config-profile-testEX3524)#upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
  ip default-gateway 192.168.13.13
  power inline compatible
  no autoinstall configuration
  no autoinstall firmware
  use firewall-policy default
  service pm sys-restart
upgrade opcode auto
upgrade opcode path  ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#
```
7.4.5 use

- EX3524 & EX3548 Profile/Device Config Commands

Applies an EX3500 management policy to this EX35XX profile

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

```
use ex3500-management-policy <POLICY-NAME>
```

**Parameters**

- use ex3500-management-policy <POLICY-NAME>

---

**Examples**

```
nx9500-6C8809(config-profile-testEX3524)#use ex3500-management-policy test
Trustpoints HTTPS Server and RSA keys for SSH can be configured with 'trustpoint' and 'rsa-key' commands in device context
```

```
nx9500-6C8809(config-profile-testEX3524)#show context
```

```
nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
  ip default-gateway 192.168.13.13
  power inline compatible
  no autoinstall configuration
  no autoinstall firmware
  interface ge 1 17
  interface ge 1 16
  interface ge 1 15
  --More--
```

```
use ex3500-management-policy test
```

```
use firewall-policy default
service pm sys-restart
upgrade opcode auto
upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
upgrade opcode reload
```

```
nx9500-6C8809(config-profile-testEX3524)#
```
7.4.6 no

EX3524 & EX3548 Profile/Device Config Commands

Removes or reverts this EX3500 profile’s settings

Supported in the following platforms:
- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX45XX, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax
no [interface vlan <1-4094>|default-gateway {<IP>}|power inline compatible|
    upgrade opcode [auto|path|reload]|use ex3500-management-policy]

Parameters
- no <PARAMETERS>

Examples
nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
  ip default-gateway 192.168.13.13
  power inline compatible
  no autoinstall configuration
  no autoinstall firmware
  interface ge 1 17
  interface ge 1 16
  interface ge 1 15
  interface ge 1 14
  interface ge 1 13
  interface ge 1 12
  interface ge 1 11
  interface ge 1 10
  interface ge 1 24
  interface ge 1 22
  interface vlan 20
  interface ge 1 23
--More--
  use ex3500-management-policy test
  use firewall-policy default
  service pm sys-restart
  upgrade opcode auto
  upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
  upgrade opcode reload

nx9500-6C8809(config-profile-testEX3524)#

nx9500-6C8809(config-profile-testEX3524)#no use ex3500-management-policy
nx9500-6C8809(config-profile-testEX3524)#no upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#no interface vlan 20

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
  ip default-gateway 192.168.13.13
  power inline compatible
  no autoinstall configuration
  no autoinstall firmware
  interface ge 1 17
  interface ge 1 16
  interface ge 1 15
  interface ge 1 14
  interface ge 1 13
  interface ge 1 12
  interface ge 1 11
  interface ge 1 10

interface ge 1 24
interface ge 1 22
interface ge 1 23

--More--
use firewall-policy default
service pm sys-restart
upgrade opcode auto
upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
nx9500-6C8809(config-profile-testEX3524)#
This chapter summarizes the Authentication, Authorization, and Accounting (AAA) policy commands in the CLI command structure.

A AAA policy enables administrators to define access control settings governing network permissions. External RADIUS and LDAP servers (AAA servers) also provide user database information and user authentication data. Each WLAN maintains its own unique AAA configuration.

AAA provides a modular way of performing the following services:

Authentication — Provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating attribute-value (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it’s applied equally to all interfaces.

Accounting — Collects and sends security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored locally on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it is applied equally to all interfaces on the access servers.
Use the (config) instance to configure AAA policy commands. To navigate to the config-aaa-policy instance, use the following commands:

```
<DEVICE>(config)#aaa-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#aaa-policy test
```
```
rfs7000-37FABE(config-aaa-policy-test)#?
```
AAA Policy Mode commands:
- **accounting**: Configure accounting parameters
- **attribute**: Configure RADIUS attributes in access and accounting requests
- **authentication**: Configure authentication parameters
- **health-check**: Configure server health-check parameters
- **mac-address-format**: Configure the format in which the MAC address must be filled in the Radius-Request frames
- **no**: Negate a command or set its defaults
- **proxy-attribute**: Configure radius attribute behavior when proxying through controller or rf-domain-manager
- **server-pooling-mode**: Configure the method of selecting a server from the pool of configured AAA servers
- **use**: Set setting to use

```
clrscr C clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
do End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-aaa-policy-test)#
```

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
8.1 aaa-policy

The following table summarizes AAA policy configuration commands:

Table 8.1 AAA-Policy-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Configures accounting parameters</td>
<td>page 8-4</td>
</tr>
<tr>
<td>attribute</td>
<td>Configure RADIUS attributes in access and accounting requests</td>
<td>page 8-8</td>
</tr>
<tr>
<td>authentication</td>
<td>Configures authentication parameters</td>
<td>page 8-11</td>
</tr>
<tr>
<td>health-check</td>
<td>Configures health check parameters</td>
<td>page 8-16</td>
</tr>
<tr>
<td>mac-address-format</td>
<td>Configures the MAC address format</td>
<td>page 8-17</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 8-18</td>
</tr>
<tr>
<td>proxy-attribute</td>
<td>Configures the RADIUS server’s attribute behavior when proxying through the wireless controller or the RF Domain manager</td>
<td>page 8-20</td>
</tr>
<tr>
<td>server-pooling-mode</td>
<td>Defines the method for selecting a server from the pool of configured AAA servers</td>
<td>page 8-21</td>
</tr>
<tr>
<td>use</td>
<td>Defines the AAA command settings</td>
<td>page 8-22</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
### 8.1.1 accounting

#### aaa-policy

Configures the server type and interval at which interim accounting updates are sent to the server. A maximum of 6 accounting servers can be configured.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
accounting [interim|server|type]
accounting interim interval <60-3600>
accounting server [<1-6>|preference]
accounting server preference [auth-server-host|auth-server-number|none]
accounting server <1-6> [dscp|host|nai-routing|onboard|proxy-mode|retry-timeout-factor|timeout]
accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]
accounting server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>]
<SECRET> | {port <1-65535>}
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT>
accounting server <1-6> onboard [centralized-controller|self|controller]
accounting server <1-6> proxy-mode [none|through-centralized-controller]
through-controller [through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]
accounting server <1-6> timeout <1-60> {attempts <1-10>}
accounting type [start-interim-stop|start-stop|stop-only]
```

#### Parameters

- **accounting interim interval <60-3600>**
  - **interim**
    - Configures the interim accounting interval
  - **interval <60-3000>**
    - Specify the interim interval from 60 - 3600 seconds. The default is 1800 seconds.

- **accounting server preference [auth-server-host|auth-server-number|none]**
  - **server**
    - Configures a RADIUS accounting server’s settings
  - **preference**
    - Configures the accounting server’s preference mode. Authentication requests are forwarded to a accounting server, from the pool, based on the preference mode selected.
  - **auth-server-host**
    - Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is identified by its hostname.
  - **auth-server-number**
    - Sets the authentication server as the accounting server. This parameter indicates the same server is used for authentication and accounting. The server is identified by its index or number.
  - **none**
    - Indicates the accounting server is independent of the authentication server
- **accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]**

<table>
<thead>
<tr>
<th>server &lt;1-6&gt;</th>
<th>Configures an accounting server. Up to 6 accounting servers can be configured.</th>
</tr>
</thead>
</table>

| dscp <0-63> | Sets the Differentiated Services Code Point (DSCP) value for Quality of Service (QOS) monitoring. This value is used in generated RADIUS packets.  
  - <0-63> – Sets the DSCP value from 0 - 63. The default value is 34. |

| retry-timeout-factor <50-200> | Sets the scaling factor for retransmission timeouts. The timeout at each attempt is a function of this retry-timeout factor and the attempt number.  
  - <50-200> – Specify a value from 50 - 200. The default is 100.  
  If the scaling factor is 100, the interval between two consecutive retries remains the same, irrespective of the number of retries.  
  If the scaling factor is less than 100, the interval between two consecutive retries reduces with subsequent retries.  
  If this scaling factor is greater than 100, the interval between two consecutive retries increases with subsequent retries. |

- **accounting server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET> | 2 <SECRET> | <SECRET>] {port <1-65535>}**

<table>
<thead>
<tr>
<th>server &lt;1-6&gt;</th>
<th>Configures an accounting server. Up to 6 accounting servers can be configured.</th>
</tr>
</thead>
</table>

| host <IP/HOSTNAME/HOST-ALIAS> | Configures the accounting server’s hostname IP address, or host-alias  
  **Note:** The host alias should be existing and configured. |

| secret [0 <SECRET> | 2 <SECRET> | <SECRET>] | Configures a common secret key used to authenticate with the accounting server  
  - 0 <SECRET> – Configures a clear text secret key  
  - 2 <SECRET> – Configures an encrypted secret key  
  - <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters. |

| port <1-65535> | Optional. Configures the accounting server’s UDP port (the port used to connect to the accounting server)  
  - <1-65535> – Sets the port number from 1 - 65535 (default port is 1813) |

- **accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT> {strip}**

<table>
<thead>
<tr>
<th>server &lt;1-6&gt;</th>
<th>Configures an accounting server. Up to 6 accounting servers can be configured.</th>
</tr>
</thead>
</table>

| nai-routing | Enables Network Access Identifier (NAI) routing. This option is disabled by default.  
  The NAI is a character string in the format of an e-mail address as either user or user@ (it need not be a valid e-mail address or a fully qualified domain name (FQDN). The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dial up ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers. |

<p>| realm-type | Specifies whether the prefix or suffix of the username is used as the match criteria. For example, if the option selected is prefix, the username’s prefix is matched to the realm. |</p>
<table>
<thead>
<tr>
<th>Prefix/Suffix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting server &lt;1-6&gt; onboard [centralized-controller</td>
<td>self</td>
</tr>
<tr>
<td>prefix</td>
<td>Matches the prefix of the username (For example, username is of type DOMAIN/user1, DOMAIN/user2). This is the default setting.</td>
</tr>
<tr>
<td>suffix</td>
<td>Matches the suffix of the username (For example, user1@DOMAIN, user2@DOMAIN)</td>
</tr>
<tr>
<td>realm &lt;REALM-TEXT&gt;</td>
<td>Configures the text matched against the username. Enter the realm name (should not exceed 50 characters). When the RADIUS accounting server receives a request for a user name, the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server.</td>
</tr>
<tr>
<td>strip</td>
<td>Optional. When enabled, strips the realm from the username before forwarding the request to the RADIUS server. This option is disabled by default.</td>
</tr>
</tbody>
</table>

- prefix – Matches the prefix of the username (For example, username is of type DOMAIN/user1, DOMAIN/user2). This is the default setting.
- suffix – Matches the suffix of the username (For example, user1@DOMAIN, user2@DOMAIN)

<table>
<thead>
<tr>
<th>Strip</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>strip</td>
<td>Optional. When enabled, strips the realm from the username before forwarding the request to the RADIUS server. This option is disabled by default.</td>
</tr>
</tbody>
</table>

- accounting server <1-6> onboard [centralized-controller|self|controller] | Select one of the following options: |
| server <1-6> | Configures an accounting server. Up to 6 accounting servers can be configured. |
| onboard | Selects an onboard server instead of an external host |
| centralized-controller | Configures the server on the centralized controller managing the network |
| self | Configures the onboard server on a AP, wireless controller, or service platform (where the client is associated) |
| controller | Configures local RADIUS server settings |

- accounting server <1-6> proxy-mode [none|through-centralized-controller|through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager] | Select the mode used to proxy requests. The options are: none, through-controller, and through-rf-domain-manager. |
| server <1-6> | Configures an accounting server. Up to 6 accounting servers can be configured. |
| proxy-mode | Select the mode used to proxy requests. The options are: none, through-controller, and through-rf-domain-manager. |
| none | No proxy required. Sends the request directly using the IP address of the device. This is the default setting. |
| through-centralized-controller | Proxy requests through the centralized controller that is configuring and managing the network |
| through-controller | Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device |
| through-mint-host <HOSTNAME/MINT-ID> | Proxies requests through a neighboring MiNT device. Provide the device’s MiNT ID or hostname. |
| through-rf-domain-manager | Proxies requests through the local RF Domain Manager |

- accounting server <1-6> timeout <1-60> {attempts <1-10>} | Configures an accounting server. Up to 6 accounting servers can be configured. |
### timeout <1-60>

Configures the timeout for each request sent to the RADIUS server
- `<1-60>` – Specify a value from 1 - 60 seconds. The default is 5 seconds.

### attempts <1-10>

Optional. Specifies the number of times a transmission request is attempted
- `<1-10>` – Specify a value from 1 - 10. The default is 3.

---

- **accounting type** [start-interim-stop|start-stop|stop-only]

### type

Configures the type of RADIUS accounting packets sent. The options are: start-interim-stop, start-stop, and stop-only.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-interim-stop</td>
<td>Sends accounting-start and accounting-stop messages when the session starts and stops. This parameter also sends interim accounting updates.</td>
</tr>
<tr>
<td>start-stop</td>
<td>Sends accounting-start and accounting-stop messages when the session starts and stops. This is the default setting.</td>
</tr>
<tr>
<td>stop-only</td>
<td>Sends an accounting-stop message when the session ends</td>
</tr>
</tbody>
</table>

---

### Examples

```bash
rfs7000-37FABE(config-aaa-policy-test)#accounting interim interval 65
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 host 172.16.10.10 secret test1 port 1
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 timeout 2 attempts 2
rfs7000-37FABE(config-aaa-policy-test)#accounting type start-stop
rfs7000-37FABE(config-aaa-policy-test)#accounting server preference auth-server-number
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
accounting server 2 host 172.16.10.10 secret 0 test1 port 1
accounting server 2 timeout 2 attempts 2
accounting interim interval 65
accounting server preference auth-server-number
rfs7000-37FABE(config-aaa-policy-test)#
```

---

### Related Commands

- **no**
  - Removes or resets accounting server parameters
8.1.2 attribute

aaa-policy

Configures RADIUS Framed-MTU attribute used in access and accounting requests. The Framed-MTU attribute reduces the Extensible Authentication Protocol (EAP) packet size of the RADIUS server. This command is useful in networks where routers and firewalls do not perform fragmentation.

To ensure network security, some firewall software drop UDP fragments from RADIUS server EAP packets. Consequently, the packets are large. Using Framed MTU reduces the packet size. EAP authentication uses Framed MTU to notify the RADIUS server about the Maximum Transmission Unit (MTU) negotiation with the client. The RADIUS server communications with the client do not include EAP messages that cannot be delivered over the network.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa|framed-ip-address|framed-mtu|location-information|nas-ipv6-address|operator-name|service-type]

attribute acct-delay-time
attribute acct-multi-session-id
attribute chargeable-user-identity
attribute cisco-vsa audit-session-id
attribute framed-ip-address
attribute framed-mtu <100-1500>
attribute location-information [include-always|none|server-requested]
attribute nas-ipv6-address
attribute operator-name <OPERATOR-NAME>
attribute service-type [framed|login]

Parameters

- attribute acct-delay-time

acct-delay-time Enables support for accounting-delay-time attribute in accounting requests. When enabled, this attribute indicates the number of seconds the client has been trying to send a request to the accounting server. By subtracting this value from the time the packet is received by the server, the system is able to calculate the time of a request-generating event. Note, the network transit time is ignored. This option is disabled by default.

Note: Including the acct-delay-time attribute in accounting requests updates the acct-delay-time value whenever the packet is retransmitted. This changes the content of the attributes field, requiring a new identifier and request authenticator.

- attribute acct-multi-session-id

acct-multi-session-id Enables support for accounting-multi-session-id attribute. When enabled, it allows linking of multiple related sessions of a roaming client. This option is useful in scenarios where a client roaming between access points sends multiple RADIUS accounting requests to different access points. This option is disabled by default.
### AAA-POLICY 8-9

- **attribute chargeable-user-identity**

  | chargeable-user-identity | Enables support for chargeable-user-identity attribute. This option is disabled by default. |

- **attribute cisco-vsa audit-session-id**

  | cisco-vsa audit-session-id | Configures the CISCO Vendor Specific Attribute (VSA) attribute included in access requests. This feature is disabled by default. This VSA allows CISCO’s Identity Services Engine (ISE) to validate a requesting client’s network compliance, such as the validity of virus definition files (antivirus software or definition files for an anti-spyware software application). |

  - **audit-session-id** – Includes the audit session ID attribute in access requests

  **Note:** The audit session ID is included in access requests when Cisco ISE is configured as an authentication server.

  **Note:** If the Cisco VSA attribute is enabled, configure an additional UDP port to listen for dynamic authorization messages from the Cisco ISE server. For more information, see [service](#).

- **attribute framed-ip-address**

  | framed-ip-address | Enables inclusion of framed IP address attribute in access requests. This option is disabled by default. |

- **attribute framed-mtu <100-1500>**

  | framed-mtu <100-1500> | Configures Framed-MTU attribute used in access requests

  - **<100-1500>** – Specify the Framed-MTU attribute from 100 - 1500. The default value is 1400.

- **attribute location-information [include-always|none|server-requested]**

  | location-information [include-always|none|server-requested] | Enables support for RFC5580 location information attribute, based on the option selected. The various options are:

  - **include-always** – Always includes location information in RADIUS authentication and accounting messages
  - **none** – Disables sending of location information in RADIUS authentication and accounting messages. This is the default setting.
  - **server-requested** – Includes location information in RADIUS authentication and accounting messages only when requested by the server

  **Note:** When enabled, location information is exchanged in authentication and accounting messages.

- **attribute nas-ipv6-address**

  | nas-ipv6-address | Enables support for NAS IPv6 address. This option is disabled by default. When enabled, IPv6 addresses are assigned to hosts. The length of IPv4 and IPv6 addresses is 32-bit and 128-bit respectively. Consequently, an IPv6 address requires a larger address space. |
**attribute operator-name <OPERATOR-NAME>**

| operator-name   | Enables support for RFC5580 operator name attribute. When enabled, the network operator’s name is included in all RADIUS authentication and accounting messages and uniquely identifies the access network owner. This option is disabled by default.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;OPERATOR-NAME&gt;</td>
<td>• &lt;OPERATOR-NAME&gt; – Specify the network operator’s name (should not exceed 63 characters in length).</td>
</tr>
</tbody>
</table>

**attribute service-type [framed|login]**

| service-type   | Configures the service-type (6) attribute value. This attribute identifies the following: the type of service requested and the type of service to be provided.  
|----------------|--------------------------------------------------|
| framed|login | • framed – Sets service-type to framed (2) in the authentication packets. When enabled, a framed protocol, Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP), is started for the client. This is the default setting.  
|       |       | • login – Sets service-type to login (1) in the authentication packets. When enabled, the client is connected to the host. |

### Examples

```plaintext
rfs7000-37FABE(config-aaa-policy-test)#attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
  accounting server 2 host 172.16.10.10 secret 0 test1 port 1  
  accounting server 2 timeout 2 attempts 2  
  accounting interim interval 65  
  accounting server preference auth-server-number
  attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#

rfs7000-37FABE(config-aaa-policy-test1)#attribute cisco-vsa audit-session-id
rfs7000-37FABE(config-aaa-policy-test1)#show context
aaa-policy test
  attribute cisco-vsa audit-session-id
rfs7000-37FABE(config-aaa-policy-test)#
```

### Related Commands

| no | Resets values or disables commands |
### 8.1.3 authentication

- **aaa-policy**

  Configures user authentication parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
authentication [eap|protocol|server]
```

```
authentication eap wireless-client [attempts <1-10>|identity-request-retry-timeout <10-5000>|identity-request-timeout <1-60>|retry-timeout-factor <50-200>|timeout <1-60>]
```

```
authentication protocol [chap|mschap|mschapv2|pap]
```

```
authentication server <1-6> [dscp|host|nac|nai-routing|onboard|proxy-mode|retry-timeout-factor|timeout]
```

```
adscp <0-63>
authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>]
```

```
{port <1-65535>}
```

```
authentication server <1-6> nac
```

```
authentication server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-NAME> {strip}
```

```
authentication server <1-6> onboard [centralized-controller|controller|self]
```

```
authentication server <1-6> proxy-mode [none|through-centralized-controller|
```

```
through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]
```

```
adscp <0-63>
authentication server <1-6> retry-timeout-factor <50-200>
```

```
authentication server <1-6> timeout <1-60> {attempts <1-10>}
```

**Parameters**

- **authentication eap wireless-client**
  - **attempts <1-10>**
    - Configures the maximum number of attempts allowed to authenticate a wireless client
      - `<1-10>` – Specify a value from 1 - 10. The default is 3.

  - **identity-request-retry-timeout <10-5000>**
    - Configures the interval, in milliseconds, after which an EAP-identity request to the wireless client is retried
      - `<10-5000>` – Specify a value from 10 - 5000 milliseconds. The default is 1000 milliseconds.

  - **identity-request-timeout <1-60>**
    - Configures the timeout, in seconds, after the last EAP-identity request message retry attempt (to allow time to manually enter user credentials)
      - `<1-60>` – Specify a value from 1 - 60 seconds. The default is 30 seconds.

  - **retry-timeout-factor <50-200>**
    - Configures the retry timeout factor
      - `<50-200>`

  - **timeout <1-60>**
    - Configures the overall authentication timeout
      - `<1-60>` – Specify a value from 1 - 60 seconds. The default is 30 seconds.

  - **eap**
    - Configures EAP authentication parameters

  - **wireless-client**
    - Configures wireless client’s EAP parameters

  - **dscp <0-63>**
    - Configures the DSCP value for the packet

  - **host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>]{port <1-65535>}**
    - Configures the host and secret for the authentication server

  - **nac**
    - Configures the NAC authentication parameters

  - **nai-routing**
    - Configures the NAI routing parameters

  - **onboard**
    - Configures the onboard authentication parameters

  - **proxy-mode**
    - Configures the proxy mode for authentication

  - **retry-timeout-factor <50-200>**
    - Configures the retry timeout factor

  - **timeout <1-60>**
    - Configures the overall authentication timeout

  - **attempts <1-10>**
    - Configures the maximum number of attempts allowed to authenticate a wireless client
      - `<1-10>` – Specify a value from 1 - 10. The default is 3.
retry-timeout-factor <50-200>  Configures the spacing between successive EAP retries
• <50-200> – Specify a value from 50 - 200. The default is 100.
  A value of 100 indicates the interval between two consecutive retries remains the same
  irrespective of the number of retries.
  A value lesser than 100 indicates the interval between two consecutive retries reduces
  with each successive retry.
  A value greater than 100 indicates the interval between two consecutive retries
  increases with each successive retry.

timeout <1-60>  Configures the interval, in seconds, between successive EAP-identity request sent to
a wireless client
• <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.

- authentication protocol [chap|mschap|mschapv2|pap]

protocol [chap|mschap|mschapv2|pap]  Configures one of the following protocols for non-EAP authentication:
• chap – Uses Challenge Handshake Authentication Protocol (CHAP)
• mschap – Uses Microsoft Challenge Handshake Authentication Protocol (MS-
  CHAP)
• mschapv2 – Uses MS-CHAP version 2
• pap – Uses Password Authentication Protocol (PAP) (default authentication protocol
  used)

- authentication server <1-6> dscp <0-63>

server <1-6>  Configures a RADIUS authentication server. Up to 6 RADIUS servers can be
configured.
• <1-6> – Specify the RADIUS server index from 1 - 6.

dscp <0-63>  Configures the Differentiated Service Code Point (DSCP) quality of service parameter
generated in RADIUS packets. The DSCP value specifies the class of service provided
to a packet, and is represented by a 6-bit parameter in the header of every IP packet.
• <0-63> – Specify the value from 0 - 63. The default is 46.

- authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2
  <SECRET>]<SECRET> [port <1-65535>]

server <1-6>  Configures a RADIUS authentication server. Up to 6 RADIUS servers can be
configured.
• <1-6> – Specify the RADIUS server index from 1 - 6.

host <IP/HOSTNAME/
  HOST-ALIAS>  Sets the RADIUS authentication server’s IP address, hostname, or host-alias
Note: The host alias should be existing and configured.

secret [0 <SECRET>|2
  <SECRET>]<SECRET>  Configures the RADIUS authentication server’s secret. This key is used to authenticate
with the RADIUS server.
• 0 <SECRET> – Configures a clear text secret
• 2 <SECRET> – Configures an encrypted secret
• <SECRET> – Specify the secret key. The shared key should not exceed 127
  characters in length.

port <1-65535>  Optional. Specifies the RADIUS authentication server’s UDP port (this port is used to
connect to the RADIUS server)
• <1-65535> – Specify a value from 1 - 65535. The default port is 1812.
**authentication server <1-6> nac**

| server <1-6> | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>  • &lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</td>
<td></td>
</tr>
</tbody>
</table>

**nac**

Enables *Network Access Control* (NAC) on the RADIUS authentication server identified by the <1-6> parameter.

Using NAC, the controller hardware and software grant access to specific network resources. NAC performs a user and client authorization check for resources that do not have a NAC agent. NAC verifies the client’s compliance with the controller’s security policy. The controller supports only the EAP/802.1x type of NAC. However, the controller also provides a means to bypass NAC authentication for client’s that do not have NAC 802.1x support (printers, phones, PDAs etc.).

**accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-NAME> {strip}**

| server <1-6> | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>  • &lt;1-6&gt; – Specifies the RADIUS server index from 1 - 6.</td>
<td></td>
</tr>
</tbody>
</table>

**nai-routing**

Enables NAI routing. When enabled, AAA servers identify clients using NAI. This option is disabled by default.

The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users in a given or without a to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dial up ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each.

**realm-type [prefix|suffix]**

Configures the realm-type used for NAI authentication

|   • prefix – Sets the realm prefix. For example, in the realm name ‘AC\JohnTalbot’, the prefix is ‘AC’ and the user name ‘JohnTalbot’.  
|   • suffix – Sets the realm suffix. For example, in the realm name ‘JohnTalbot@AC.org’ the suffix is ‘AC.org’ and the user name is ‘JohnTalbot’.                                    |

**realm <REALM-NAME>**

Sets the realm information used for RADIUS authentication. The realm name should not exceed 64 characters in length. When the wireless controller or access point’s RADIUS server receives a request for a user name the server references a table of usernames. If the user name is known, the server proxies the request to the RADIUS server.

|   • <REALM-NAME> – Sets the realm used for authentication. This value is matched against the user name provided for RADIUS authentication. Example: 
| Preffix - AC\JohnTalbot  
| Suffix - JohnTalbot@AC.org |
strip
Optional. Indicates the realm name must be stripped from the user name before sending it to the RADIUS server for authentication. For example, if the complete username is ‘AC\JohnTalbot’, then with the strip parameter enabled, only the ‘JohnTalbot’ part of the complete username is sent for authentication. This option is disabled by default.

- authentication server <1-6> onboard [centralized-controller|controller|self]

server <1-6>
Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.
- <1-6> – Specify the RADIUS server index from 1 - 6.

onboard
[centralized-controller|controller|self]
Selects the onboard RADIUS server for authentication instead of an external host
- centralized-controller – Configures the server on the centralized controller managing the network
- controller – Configures the wireless controller, to which the AP is adopted, as the onboard wireless controller
- self – Configures the onboard server on the device (AP or wireless controller) where the client is associated as the onboard wireless controller

- authentication server <1-6> proxy-mode [none|through-centralized-controller|through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]

server <1-6>
Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.
- <1-6> – Sets the RADIUS server index between 1 - 6

proxy-mode
Configures the mode for proxying a request
- none – Proxying is not done. The packets are sent directly using the IP address of the device. This is the default setting.
- through-centralized-controller – Traffic is proxied through the centralized controller that is configuring and managing the network.
- through-controller – Traffic is proxied through the wireless controller configuring this device.
- through-mint-host <HOSTNAME/MINT-ID> – Traffic is proxied through a neighboring MiNT device. Provide the device’s hostname or MiNT ID.
- through-rf-domain-manager – Traffic is proxied through the local RF Domain manager.

- authentication server <1-6> retry-timeout-factor <50-200>

server <1-6>
Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.
- <1-6> – Specify the RADIUS server index from 1 - 6.

retry-timeout-factor
<50-200>
Configures the scaling of timeouts between two consecutive RADIUS authentication retries
- <50-200> – Specify the scaling factor from 50 - 200. The default is 100.
A value of 100 indicates the interval between two consecutive retries remains the same irrespective of the number of retries.
A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry.
A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.
• authentication server <1-6> timeout <1-60> {attempts <1-10>}

| server <1-6> | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.  
|             | • <1-6> – Specify the RADIUS server index from 1 - 6. |
| timeout <1-60> | Configures the timeout, in seconds, for each request sent to the RADIUS server. This is the time allowed to elapse before another request is sent to the RADIUS server. If a response is received from the RADIUS server within this time, no retry is attempted.  
|             | • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds. |
| attempts <1-10> | Optional. Indicates the number of retry attempts to make before giving up  
|             | • <1-10> – Specify a value from 1 -10. The default is 3. |

Examples
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 host 172.16.10.10 secret 0 test1 port 1
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 timeout 10 attempts 3
rfs7000-37FABE(config-aaa-policy-test)#authentication protocol chap
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
    authentication server 5 host 172.16.10.10 secret 0 test1 port 1
    authentication server 5 timeout 10
    accounting server 2 host 172.16.10.10 secret 0 test1 port 1
    accounting server 2 timeout 2 attempts 2
    authentication protocol chap
    accounting interim interval 65
    accounting server preference auth-server-number
    attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#

Related Commands

no | Resets authentication parameters on this AAA policy
8.1.4 health-check

- aaa-policy

An AAA server could go offline. When a server goes offline, it is marked as down. This command configures the interval after which a server marked as down is checked to see if it has come back online and is reachable.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
health-check interval <60-86400>

Parameters
- health-check interval <60-86400>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval &lt;60-86400&gt;</td>
<td>Configures an interval (in seconds) after which a down server is checked to see if it is reachable again</td>
</tr>
<tr>
<td></td>
<td>&lt;60-86400&gt; – Specify a value from 60 - 86400 seconds. The default is 3600 seconds.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-aaa-policy-test)#health-check interval 4000
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
  authentication server 5 host 172.16.10.10 secret 0 test1 port 1
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 test1 port 1
  accounting server 2 timeout 2 attempts 2
  authentication protocol chap
  accounting interim interval 65
  accounting server preference auth-server-number
  health-check interval 4000
  attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the health-check interval for AAA servers</td>
</tr>
</tbody>
</table>
8.1.5 mac-address-format

aaa-policy

Configures the format MAC addresses are filled in RADIUS request frames

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
case [lower|upper] attributes [all|username-password]
```

Parameters

- `mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]`
- `case [lower|upper] attributes [all|username-password]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>middle-hyphen</td>
<td>Configures the MAC address format as AABBC-DDEEFF</td>
</tr>
<tr>
<td>no-delim</td>
<td>Configures the MAC address format as AABBCDDEEFF (without delimiters)</td>
</tr>
<tr>
<td>pair-colon</td>
<td>Configures the MAC address format as AA:BB:CC:DD:EE:FF</td>
</tr>
<tr>
<td>pair-hyphen</td>
<td>Configures the MAC address display format as AA-BB-CC-DD-EE-FF (default setting)</td>
</tr>
<tr>
<td>quad-dot</td>
<td>Configures the MAC address display format as AABB.CCDD.EEFF</td>
</tr>
<tr>
<td>case [lower</td>
<td>upper]</td>
</tr>
<tr>
<td></td>
<td>• lower – Indicates MAC address is in lower case. For example, aa:bb:cc:dd:ee:ff</td>
</tr>
<tr>
<td></td>
<td>• upper – Indicates MAC address is in upper case. For example, AA:BB:CC:DD:EE:FF (default setting)</td>
</tr>
<tr>
<td>attributes [all</td>
<td>username-password]</td>
</tr>
<tr>
<td></td>
<td>• all – Applies to all attributes with MAC addresses such as username, password, calling-station-id, and called-station-id</td>
</tr>
<tr>
<td></td>
<td>• username-password – Applies only to the username and password fields (default setting)</td>
</tr>
</tbody>
</table>

Examples

```plaintext
rfs7000-37FABE(config-aaa-policy-test)#mac-address-format quad-dot case upper attributes username-password
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
authentication server 5 host 172.16.10.10 secret 0 test1 port 1
authentication server 5 timeout 10
accounting server 2 host 172.16.10.10 secret 0 test1 port 1
accounting server 2 timeout 2 attempts 2
mac-address-format quad-dot case upper attributes username-password
authentication protocol chap
-- More --
rfs7000-37FABE(config-aaa-policy-test)#
```

Related Commands

```plaintext
no
```
Resets the MAC address format to default (pair-hyphen)
8.1.6 no

Negates a AAA policy command or sets its default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [accounting|attribute|authentication|health-check|mac-address-format|proxy-attribute|server-pooling-mode|use]

no accounting interim interval
no accounting server preference
no accounting server <1-6> {dscp|nai-routing|proxy-mode|retry-timeout-factor|timeout}
no accounting type

no attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa audit-session-id|framed-ip-address|framed-mtu|location-information|nas-ipv6-address|operator-name|service-type]

no authentication [eap|protocol|server]
no authentication eap wireless-client [attempts|identity-request-retry-timeout|identity-request-timeout|retry-timeout-factor|timeout]
no authentication protocol
no authentication server <1-6> {dscp|nac|nai-routing|proxy-mode|retry-timeout-factor|timeout}

no health-check interval
no mac-address-format
no proxy-attribute [nas-identifier|nas-ip-address]
no server-pooling-mode
no use nac-list

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Negates a AAA policy command or sets its default |

Examples

The following example shows the AAA policy ‘test’ settings before the ‘no’ commands are executed:

rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
  authentication server 5 host 172.16.10.10 secret 0 test1 port 1
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 test1 port 1
  accounting server 2 timeout 2 attempts 2
  mac-address-format quad-dot case upper attributes username-password
  authentication protocol chap
  accounting interim interval 65
  accounting server preference auth-server-number
  health-check interval 4000
  attribute framed-mtu 110
rfs7000-37FABE(config-aaa-policy-test)#
The following example shows the AAA policy 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
  authentication server 5 host 172.16.10.10 secret 0 test1 port 1
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 test1 port 1
  mac-address-format quad-dot case upper attributes username-password
  accounting server preference auth-server-number
  health-check interval 4000
rfs7000-37FABE(config-aaa-policy-test)#
```
8.1.7 proxy-attribute

Configures RADIUS server’s attribute behavior when proxying through a wireless controller or a RF Domain manager.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6662, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
proxy-attribute [nas-identifier|nas-ip-address]
proxy-attribute [nas-identifier [originator|proxier]|nas-ip-address [none|proxier]]

Parameters
- proxy-attribute [nas-identifier [originator|proxier]|nas-ip-address [none|proxier]]

| nas-identifier [originator|proxier] | Uses NAS identifier |
|------------------------------------|---------------------|
| • originator – Configures the NAS identifier as the originator of the RADIUS request. The originator could be an AP, or a wireless controller with radio. This is the default setting. |
| • proxier – Configures the proxying device as the NAS identifier. The device could be a controller or a RF Domain manager. |

| nas-ip-address [none|proxier] | Uses NAS IP address |
|-----------------------------|---------------------|
| • none – NAS IP address attribute is not filled |
| • proxier – NAS IP address is filled by the proxying device. The device could be a controller or a RF Domain manager. This is the default setting. |

Examples
rfs7000-37FABE(config-aaa-policy-test)#proxy-attribute nas-ip-address proxier
rfs7000-37FABE(config-aaa-policy-test)#proxy-attribute nas-identifier originator

Related Commands
- no
  Resets RADIUS server’s proxying attributes
### 8.1.8 server-pooling-mode

Configures the server selection method from a pool of AAA servers. The available methods are *failover* and *load-balance*.

In the failover scenario, when a configured AAA server goes down, the server with the next higher index takes over for the failed server.

In the load-balance scenario, when a configured AAA server goes down, the remaining servers distribute the load amongst themselves.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
server-pooling-mode [failover|load-balance]
```

**Parameters**
- `server-pooling-mode [failover|load-balance]`

<table>
<thead>
<tr>
<th>failover</th>
<th>Sets the pooling mode to failover. This is the default setting. When a configured AAA server fails, the server with the next higher index takes over the failed server’s load.</th>
</tr>
</thead>
<tbody>
<tr>
<td>load-balance</td>
<td>Sets the pooling mode to load balancing When a configured AAA server fails, all servers in the pool share the failed server’s load transmitting requests in a round-robin fashion.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-aaa-policy-test)#server-pooling-mode load-balance
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
    authentication server 5 host 172.16.10.10 secret 0 test2 port 1
    authentication server 5 timeout 10
    accounting server 2 host 172.16.10.10 secret 0 test1 port 1
server-pooling-mode load-balance
    mac-address-format quad-dot case upper attributes username-password
    accounting server preference auth-server-number
    health-check interval 4000
rfs7000-37FABE(config-aaa-policy-test)#
```

**Related Commands**

- `no` | Resets the method of selecting a server, from the pool of configured AAA servers |
### 8.1.9 use

*aaa-policy*

Associates a *Network Access Control* (NAC) with this AAA policy. This allows only the set of configured devices to use the configured AAA servers.

For more information on creating a NAC list, see `nac-list`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use nac-list <NAC-LIST-NAME>
```

**Parameters**

- `use nac-list <NAC-LIST-NAME>`

**Examples**

```
rfs7000-37FABE(config-aaa-policy-test)#use nac-list test1
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
   authentication server 5 host 172.16.10.10 secret 0 test1 port 1
   authentication server 5 timeout 10
   accounting server 2 host 172.16.10.10 secret 0 test1 port 1
   server-pooling-mode load-balance
   mac-address-format quad-dot case upper attributes username-password
   accounting server preference auth-server-number
   health-check interval 4000
   use nac-list test1
rfs7000-37FABE(config-aaa-policy-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets set values or disables commands</td>
</tr>
<tr>
<td><code>nac-list</code></td>
<td>Creates a NAC list</td>
</tr>
</tbody>
</table>
CHAPTER 9
AUTO-PROVISIONING-POLICY

This chapter summarizes the auto provisioning policy commands in the CLI command structure.

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt multiple access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device uses auto provisioning policies to determine which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Auto provisioning or adoption is the process by which an access point discovers controllers in the network, identifies the most desirable controller, associates with the identified controller, and optionally obtains an image upgrade, obtains its configuration and considers itself provisioned.

At adoption, an access point solicits and receives multiple adoption responses from controllers available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller for adoption. An auto-provisioning policy maps a new AP to a profile and RF Domain based on various parameters related to the AP and where it is connected. By default a new AP will be mapped to the default profile and default RF Domain. Modify existing auto-provisioning policies or create a new one as needed to meet the configuration requirements of a device.

An auto-provisioning policy enables an administrator to define rules for the supported access points capable of being adopted by a controller. The policy determines which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CISCO Discovery Protocol (CDP) snoop strings, etc. Once created an auto provisioning policy can be used in profiles or device configuration objects. The policy contains a set of rules (ordered by precedence) that either deny or allow adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

For example,

rule #1 adopt ap7131 10 profile default vlan 10
rule #2 adopt ap650 20 profile default vlan 20
rule #3 adopt ap7131 30 profile default serial-number
rule #4 adopt ap7131 40 p d mac aa bb

AP7131 L2 adoption, VLAN 10 - will use rule #1
AP7131 L2 adoption, VLAN 20 - will not use rule #2 (wrong type), may use rule #3 if the serial number matched, or rule #4
If aa<= MAC <= bb, or else default.

With the implementation of the hierarchically managed (HM) network, the auto-provisioning policy has been modified to enable controllers to adopt other controllers in addition to access points.
The new WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single Network Operations Center (NOC) controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

All adopted devices (access points and second-level controllers) are referred to as the ‘adoptees’. The adopting devices are the ‘adopters’.

A controller cannot be configured as an adoptee and a controller adopter simultaneously. In other words, a controller can either be an adopter (adopts another controller) or an adoptee (is adopted by another controller). Therefore, a site controller, which has been adopted by a NOC controller, cannot adopt another controller. But it can adopt access points. For more information on HM network, see device-upgrade.

A controller should be configured to specify the device types (APs and/or controllers) that it can adopt. For more information on configuring the adopted-device types for a controller, see service.

**NOTE:** The adoption capabilities of a controller depends on:

- Whether the controller is deployed at the NOC or site
- A NOC controller can adopt site controllers and access points
- A site controller can adopt access points only
- The controller device type, which determines the number and type of devices it can adopt

The NOC controller can adopt a site controller with a capacity equal to or lower than its own. The following table displays the NOC controllers and the corresponding site-level controllers supported by each:

<table>
<thead>
<tr>
<th>Site Controllers supported by each NOC controller</th>
<th>NOC Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RFS7000</td>
</tr>
<tr>
<td>RFS4000</td>
<td>X</td>
</tr>
<tr>
<td>RFS6000</td>
<td>X</td>
</tr>
<tr>
<td>RFS7000</td>
<td>X</td>
</tr>
<tr>
<td>NX45XX</td>
<td>-</td>
</tr>
<tr>
<td>NX65XX</td>
<td>-</td>
</tr>
<tr>
<td>NX7500</td>
<td>-</td>
</tr>
<tr>
<td>NX9000</td>
<td>-</td>
</tr>
<tr>
<td>NX95XX</td>
<td>-</td>
</tr>
</tbody>
</table>

**NOTE:** Some access points can be configured as virtual controllers. When configured as a virtual controller, an AP can only adopt another AP of the same type. In such a scenario, an auto provisioning policy is required to enable adoption of a specific device identified by its MAC address, IP address, serial number, model number etc.
Use the (config) instance to configure an auto-provisioning policy. To navigate to the auto-provisioning-policy configuration instance, use the following command:

<DEVICE>(config)#auto-provisioning-policy <POLICY-NAME>

rfs7000-37FABE(config)#auto-provisioning-policy test
rfs7000-37FABE(config-auto-provisioning-policy-test)#?

Auto-Provisioning Policy Mode commands:

- adopt: Add rule for device adoption
- default-adoption: Adopt devices even when no matching rules are found. Assign default profile and default rf-domain
- deny: Add rule to deny device adoption
- evaluate-always: Set the flag to evaluate the policy every time, regardless of previous adoption status
- no: Negate a command or set its defaults
- redirect: Add rule to redirect device adoption
- upgrade: Add rule for device upgrade
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

rfs7000-37FABE(config-auto-provisioning-policy-test)#

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
## 9.1 auto-provisioning-policy

**AUTO-PROVISIONING-POLICY**

The following table summarizes auto provisioning policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopt</td>
<td>Adds a permit adoption rule</td>
<td>page 9-5</td>
</tr>
<tr>
<td>default-adoption</td>
<td>Adopts devices even when no matching rules are found. Assigns default profile and default RF Domain</td>
<td>page 9-10</td>
</tr>
<tr>
<td>deny</td>
<td>Adds a deny adoption rule</td>
<td>page 9-11</td>
</tr>
<tr>
<td>evaluate-always</td>
<td>Runs this policy every time a device is adopted</td>
<td>page 9-14</td>
</tr>
<tr>
<td>redirect</td>
<td>Adds a rule redirecting device adoption to a specified controller within the system</td>
<td>page 9-15</td>
</tr>
<tr>
<td>upgrade</td>
<td>Adds a device upgrade rule to this auto provisioning policy</td>
<td>page 9-19</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 9-22</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *Chapter 5, COMMON COMMANDS.*
9.1.1 adopt

Add device adoption rules

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
adopt [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]
```

```
adopt [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[profile|rf-domain]
```

```
adopt [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any
```

```
```

Parameters:
- adopt [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any

```
adopt [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any
```

Adopt

Adding an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.

The different device types are: anyap, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX7500, NX7510, NX7520, NX7530, NX9000, VX9000, and NX9600.

Note: ‘anyap’ is used in auto provisioning policies to create rules that are applicable to any AP regardless of the type.

Parameters:
- adopt [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any

precedence <1-10000>

Sets the rule precedence from 1 - 10000. A rule with a lower value has a higher precedence.
### profile <DEVICE-PROFILE-NAME>
Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an AP650 device profile for an AP650. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name.
Provide a device profile name. Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor'.
Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system.

### rf-domain <RF-DOMAIN-NAME>
Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name OR use a string alias to identify the RF Domain.
Provide the full RF Domain name or an alias. Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]'
Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system.

**Note:** Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.example_company.com'. In this example, the string-alias $DOMAIN is mapped to the string: *test.example_company.com*. For more information, see alias.

### any
Indicates any device. Any device seeking adoption is adopted.

### adopt [anyap | ap621 | ap622 | ap650 | ap6511 | ap6521 | ap6522 | ap6532 | ap6562 | ap71xx | ap7502 | ap7522 | ap7532 | ap7562 | ap81xx | ap82xx | ap81xx | rfs4000 | rfs6000 | rfs7000 | nx45xx | nx5000 | nx55xx | nx9000 | vx9000 | nx9600] precedence <1-10000> [profile <DEVICE-PROFILE-NAME>] rf-domain <RF-DOMAIN-NAME> [area <AREA-NAME>] [cdp-match <LOCATION-SUBSTRING>] [dhcp-option <DHCPOPTION>] [floor <FLOOR-NAME>] [fqdn <FQDN>] [ip <IP/START-IP> <IP/MASK> | <END-IP> <IP/MASK>] [lldp-match <LLDP-STRING>] [mac <START-MAC> <END-MAC>] [<MODEL-NUMBER>] [serial-number <SERIAL-NUMBER>] [rf-domain <RF-DOMAIN-NAME>] [vlan <VLAN-ID>]

### adopt
Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.
The different device types are: anyap, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP7502, AP7522, AP7532, AP7562, AP71XX, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5000, NX55XX, NX65XX, NX7500, NX7510, NX7520, NX7530, NX9000, Vx9000, and NX9600.
**Note:** 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the type.

### precedence <1-10000>
Sets the rule precedence. A rule with a lower value has a higher precedence.

### profile <DEVICE-PROFILE-NAME>
Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an AP650 device profile for an AP650. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name. Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor'.
Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rf-domain &lt;RF-DOMAIN-NAME&gt;</td>
<td>Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name or an alias. Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]'. Please see the Usage Guidelines section Built-in Tokens &amp; Alias for the different types of built in tokens available in the system. <strong>Note:</strong> Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.example_company.com'. In this example, the string-alias $DOMAIN is mapped to the string: test.example_company.com. For more information, see alias.</td>
</tr>
<tr>
<td>area &lt;AREA-NAME&gt;</td>
<td>Matches the area of deployment. This option is not applicable to the ‘rf-domain’ parameter.</td>
</tr>
<tr>
<td></td>
<td>• &lt;AREA-NAME&gt; – Enter a 64 character maximum deployment area name assigned to this policy. Devices with matching area names are adopted.</td>
</tr>
<tr>
<td>cdp-match &lt;LOCATION-SUBSTRING&gt;</td>
<td>Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com, 'controller1', 'example', 'example.com', are examples of the substrings that will match.</td>
</tr>
<tr>
<td></td>
<td>• &lt;LOCATION-SUBSTRING&gt; – Specify the value to match. Devices matching the specified value are adopted.</td>
</tr>
<tr>
<td>dhcp-option &lt;DHCP-OPTION&gt;</td>
<td>Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present.</td>
</tr>
<tr>
<td></td>
<td>• &lt;DHCP-OPTION&gt; – Specify the DHCP option. Devices matching the specified value are adopted.</td>
</tr>
<tr>
<td>floor &lt;FLOOR-NAME&gt;</td>
<td>Matches the floor name. This option is not applicable to the ‘rf-domain’ parameter.</td>
</tr>
<tr>
<td></td>
<td>• &lt;FLOOR-NAME&gt; – Enter a 32 character maximum deployment floor name assigned to this policy. Devices with matching floor names are adopted.</td>
</tr>
<tr>
<td>fqdn &lt;FQDN&gt;</td>
<td>Matches a substring to the Fully Qualified Domain Name (FQDN) of a device (case insensitive)</td>
</tr>
<tr>
<td></td>
<td>FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. This parameter allows a device to adopt based on its FQDN value.</td>
</tr>
<tr>
<td></td>
<td>• &lt;FQDN&gt; – Specify the FQDN. Devices matching the specified value are adopted.</td>
</tr>
<tr>
<td>ip [&lt;START-IP&gt; [END-IP&gt; [&lt;IP/MASK&gt;]]</td>
<td>Adopts a device if its IP address matches the specified IPv4 address or is within the specified IP address range. Or if the device is a part of the specified subnet.</td>
</tr>
<tr>
<td></td>
<td>• &lt;START-IP&gt; – Specify the first IPv4 address in the range.</td>
</tr>
<tr>
<td></td>
<td>• &lt;END-IP&gt; – Specify the last IPv4 address in the range.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP/MASK&gt; – Specify the IPv4 subnet and mask to match against the device’s IP address.</td>
</tr>
</tbody>
</table>
### ipv6

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;START-IP&gt;</code> &lt;END-IP&gt;</td>
<td>Adopts a device if its IP v6 address matches the specified IPv6 address or is within the specified IP address range. Or if the device is a part of the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;IP/MASK&gt;</code></td>
<td>• <code>&lt;START-IP&gt;</code> – Specify the first IPv6 address in the range.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;END-IP&gt;</code> – Specify the last IPv6 address in the range.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP/MASK&gt;</code> – Specify the IPv6 subnet and mask to match against the device’s IPv6 address.</td>
</tr>
</tbody>
</table>

### lldp-match

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;LLDP-STRING&gt;</code></td>
<td>Matches a substring in a list of Link Layer Discovery Protocol (LLDP) snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com,'controller1', 'example', 'example.com', are examples of the substrings that will match. LLDP is a vendor neutral link layer protocol that advertises a network device’s identity, capabilities, and neighbors on a local area network.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;LLDP-STRING&gt;</code> – Specify the LLDP string. Devices matching the specified value are adopted.</td>
</tr>
</tbody>
</table>

### mac

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;START-MAC&gt;</code> {&lt;END-MAC}&gt;</td>
<td>Adopts a device if its MAC address matches the specified MAC address or is within the specified MAC address range</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;START-MAC&gt;</code> – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;END-MAC&gt;</code> – Optional. Specify the last MAC address in the range.</td>
</tr>
</tbody>
</table>

### model-number

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MODEL-NUMBER&gt;</code></td>
<td>Adopts a device if its model number matches <code>&lt;MODEL-NUMBER&gt;</code></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;MODEL-NUMBER&gt;</code> – Specify the model number.</td>
</tr>
</tbody>
</table>

### rf-domain

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RF-DOMAIN-NAME&gt;</code></td>
<td>Adopts a device if its RF Domain matches <code>&lt;RF-DOMAIN-NAME&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;RF-DOMAIN-NAME&gt;</code> – Specify the RF Domain name. You can use a string alias to specify a RF Domain.</td>
</tr>
<tr>
<td></td>
<td>Provide the full RF Domain name or an alias. Or a template with appropriate substitution tokens, such as <code>$CDP[1:7]</code>, <code>$DNS-SUFFIX[1:5]</code></td>
</tr>
<tr>
<td></td>
<td>Please see the Usage Guidelines section Built-in Tokens &amp; Alias for the different types of built in tokens available in the system.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use the built-in string alias or a user-defined string alias. String aliases allow you</td>
</tr>
<tr>
<td></td>
<td>to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, ‘alias string $DOMAIN test.example_company.com’. In this example, the string-alias $DOMAIN is mapped to the string: test.example_company.com. For more information, see alias.</td>
</tr>
</tbody>
</table>

### serial-number

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;SERIAL-NUMBER&gt;</code></td>
<td>Adopts a device if its serial number matches <code>&lt;SERIAL-NUMBER&gt;</code></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;SERIAL-NUMBER&gt;</code> – Specify the serial number.</td>
</tr>
</tbody>
</table>

### vlan

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;VLAN-ID&gt;</code></td>
<td>Adopts a device if its VLAN matches <code>&lt;VLAN-ID&gt;</code></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;VLAN-ID&gt;</code> – Specify the VLAN ID.</td>
</tr>
</tbody>
</table>
Usage Guidelines Built-in Tokens & Alias

Following are the built-in tokens that can be used to identify the devices to adopt:

$FQDN  - references FQDN of adopting device  
$CDP   - references CDP Device Id of wired switch to which adopting device is connected  
$LLDP  - references LLDP System Name of wired switch to which adopting device is connected  
$DHCP  - references DHCP Option Value received by the adopting device  
$SN    - references SERIAL NUMBER of adopting device  
$MODEL - references MODEL NUMBER of adopting device  
$DNS-SUFFIX - references FQDN excluding the hostname of the adopting device  
$CDP-SUFFIX - references CDP excluding the hostname of the adopting device  
$LLDP-SUFFIX - references LLDP excluding the hostname of the adopting device

Following is the built-in alias that can be used to identify the RF Domain of devices to adopt:

$_builtin_rf-domain - rf-domain of adopting device

Examples

rfs4000-229D58(config-auto-provisioning-policy-test)#adopt ap81xx precedence 1 profile default-ap81xx vlan 1  
rfs4000-229D58(config-auto-provisioning-policy-test)#show context auto-provisioning-policy test  
  adopt ap81xx precedence 1 profile default-ap81xx vlan 1  
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#show wireless ap configured  
---------------------------------------------------------------------------------------  
IDX   NAME              MAC             PROFILE       RF-DOMAIN       ADOPTED-BY       
---------------------------------------------------------------------------------------  
1      ap81xx-711728    B4-C7-99-71-17-28   default-ap81xx   default   00-23-68-22-9D-58  
2      rfs4000-229D58   00-23-68-22-9D-58   default-rfs4000  default
---------------------------------------------------------------------------------------
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs7000-6DCD4B(config-auto-provisioning-policy-test)#adopt anyap precedence 1 profile rfs7000 any

rfs7000-6DCD4B(config-auto-provisioning-policy-test)#show context auto-provisioning-policy test  
  adopt anyap precedence 1 profile rfs7000 any
rfs7000-6DCD4B(config-auto-provisioning-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an adopt rule</td>
</tr>
</tbody>
</table>
9.1.2 default-adoption

Adopts devices, even when no matching rules are defined, and assigns a default profile and default RF Domain to the adopted device

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

default-adoption

Parameters

None

Examples

rfs4000-229D58(config-auto-provisioning-policy-test)#default-adoption

rfs4000-229D58(config-auto-provisioning-policy-test)#show context auto-provisioning-policy test

default-adoption

default-adoption

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables adoption of devices when matching rules are not found</td>
</tr>
</tbody>
</table>
### 9.1.3 deny

**auto-provisioning-policy**

Defines a deny device adoption rule

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

deny [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]
deny [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> [any|cdp-match|dhcp-option|fqdn|ip|ipv6|lldp-match|mac|model-number|serial-number|vlan]
deny [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any


**Parameters**

- deny [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any

**deny**

Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.

The different device types are: anyap, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, VX9000, and NX9600 series.

**Note:** 'anyap' is used in auto provisioning policies to create rules that are applicable to any regardless of the type.

**precedence**

Sets the rule precedence. A rule with a lower value has a higher precedence.

**any**

Indicates any device. Any device seeking adoption is denied adoption.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX56XX, NX75XX, NX9000, VX9000, and NX9600.</td>
</tr>
<tr>
<td>precedence &lt;1-10000&gt;</td>
<td>Sets the rule precedence. A rule with a lower value has a higher precedence. After specifying the rule precedence, specify the match criteria. Devices matching the specified criteria are denied adoption.</td>
</tr>
<tr>
<td>cdp-match &lt;LOCATION-SUBSTRING&gt;</td>
<td>Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com, 'controller1', 'example', 'example.com', are examples of the substrings that will match.</td>
</tr>
<tr>
<td>dhcp-option &lt;DHCP-OPTION&gt;</td>
<td>Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present.</td>
</tr>
<tr>
<td>fqdn &lt;FQDN&gt;</td>
<td>Matches a substring to the FQDN of a device (case insensitive) FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain.</td>
</tr>
<tr>
<td>ip [&lt;START-IP&gt;</td>
<td>&lt;END-IP&gt;</td>
</tr>
<tr>
<td>ipv6 [&lt;START-IP&gt;</td>
<td>&lt;END-IP&gt;</td>
</tr>
</tbody>
</table>
AUTO-PROVISIONING-POLICY 9-13

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>lldp-match</strong>&lt;LLDP-STRING&gt;</td>
<td>Matches a substring in a list of LLDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com,'controller1', 'example', 'example.com', are examples of the substrings that will match. LLDP is a vendor neutral link layer protocol used to advertise a network device’s identity, capabilities, and neighbors on a local area network. • &lt;LLDP-STRING&gt; – Specify the LLDP string. Devices matching the specified values are denied adoption.</td>
</tr>
<tr>
<td><strong>mac</strong>&lt;START-MAC&gt;{&lt;END-MAC&gt;}</td>
<td>Denies adoption if a device’s MAC address matches the specified MAC address or is within the specified MAC address range • &lt;START-MAC&gt; – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device. • &lt;END-MAC&gt; – Optional. Specify the last MAC address in the range.</td>
</tr>
<tr>
<td><strong>model-number</strong>&lt;MODEL-NUMBER&gt;</td>
<td>Denies adoption if a device’s model number matches &lt;MODEL-NUMBER&gt; • &lt;MODEL-NUMBER&gt; – Specify the model number.</td>
</tr>
<tr>
<td><strong>serial-number</strong>&lt;SERIAL-NUMBER&gt;</td>
<td>Denies adoption if a device’s serial number matches &lt;SERIAL-NUMBER&gt; • &lt;SERIAL-NUMBER&gt; – Specify the serial number.</td>
</tr>
<tr>
<td><strong>vlan</strong>&lt;VLAN-ID&gt;</td>
<td>Denies adoption if a device’s VLAN matches &lt;VLAN-ID&gt; • &lt;VLAN-ID&gt; – Specify the VLAN ID.</td>
</tr>
</tbody>
</table>

**Examples**

rfs4000-229D58(config-auto-provisioning-policy-test)#deny ap71xx precedence 2 model-number AP7131N

rfs4000-229D58(config-auto-provisioning-policy-test)#deny ap71xx precedence 3 ip 192.168.13.23 192.168.13.23

rfs4000-229D58(config-auto-provisioning-policy-test)#show context auto-provisioning-policy-test
  adopt ap81xx precedence 1 profile default-ap81xx vlan 1
deny ap71xx precedence 2 model-number AP7131N
deny ap71xx precedence 3 ip 192.168.13.23 192.168.13.23
rfs4000-229D58(config-auto-provisioning-policy-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes a deny adoption rule</td>
</tr>
</tbody>
</table>
9.1.4 evaluate-always

- auto-provisioning-policy

Sets flag to run this auto-provisioning policy every time an access point is adopted. The access point's previous adoption status is not taken into consideration.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510,NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
evaluate-always

Parameters
None

Examples
rfs4000-229D58(config-auto-provisioning-policy-test)#evaluate-always

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
evaluate-always
rfs4000-229D58(config-auto-provisioning-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the running of this policy every time an AP is adopted</td>
</tr>
</tbody>
</table>
9.1.5 redirect

**auto-provisioning-policy**

Adds a rule redirecting device adoption to another controller within the system. Devices seeking adoption are redirected to a specified controller based on the redirection parameters specified.

**Syntax**

```
redirect [anyap|ap621|ap622|ap650|ap651|ap652|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]
```

```
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>]
```

```
[any|cdp-match|dhcp-option|fqdn|ip|ipv6|level|lldp-match|mac|model-number|pool<1-2>|serial-number|vlan]
```

**Parameters**

- **redirect [anyap|ap621|ap622|ap650|ap651|ap652|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any

- **redirect [anyap|ap621|ap622|ap650|ap651|ap652|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6]

**redirect** Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.

The different device types are: anyap, AP621, AP622, AP650, AP651, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, VX9000, NX9600 series.

**Note:** ‘anyap’ is used in auto provisioning policies to create rules that are applicable to any AP regardless of the type.

**Note:** An adoptee controller, such as RFS4000, RFS6000, and RFS7000, can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see **controller**.

**precedence <1-10000>** Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
### 9-16 WiNG 5.8.1 CLI Reference Guide

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `controller` `<CONTROLLER-IP>` `<CONTROLLER-HOSTNAME>` `|ipv6>` | Configures the controller to which the adopting devices are redirected. Specify the controller’s IP address or hostname.  
- `<CONTROLLER-IP>` – Specifies the controller’s IP address  
- `<CONTROLLER-HOSTNAME>` – Specifies the controller’s hostname  
- `ipv6` – Specify the controller’s IPv6 address |
| `any` | Indicates any device. Any device seeking adoption is redirected. |
| `redirect` `<CONTROLLER-IP>` `<CONTROLLER-HOSTNAME>` `|ipv6>` | Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.  
- The different device type options are: anyap, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX5510, NX75XX, NX7530, NX9000, VX9000, VX9600  
- `<LOCATION-SUBSTRING>` – Specify the location. Devices matching the specified string are redirected.  
- `<DHCP-OPTION>` – Specify the DHCP option value. Devices matching the specified option value are redirected.  
- `<FQDN>` – Specify the FQDN. Devices matching the specified value are redirected.  
- `<MODEL-NUMBER>` – Specify the model number. Devices matching the specified value are redirected.  
- `<VLAN-ID>` – Specify the VLAN ID. Devices matching the specified value are redirected. |
| `precedence `<1-1000>` | Sets the rule precedence. Rules with lower values get precedence over rules with higher values. |
| `controller` `<CONTROLLER-IP>` `<CONTROLLER-HOSTNAME>` `|ipv6>` | Configures the controller to which the adopting devices are redirected. Specify the controller’s IP address or hostname.  
- `<CONTROLLER-IP>` – Specifies the controller’s IP address  
- `<CONTROLLER-HOSTNAME>` – Specifies the controller’s hostname  
- `ipv6` – Specify the controller’s IPV6 address. |
| `cdp-match` `<LOCATION-SUBSTRING>` | Configures the device location to match, based on CDP snoop strings  
- `<LOCATION-SUBSTRING>` – Specify the location. Devices matching the specified string are redirected. |
| `dhcp-option` `<DHCP-OPTION>` | Configures the DHCP options to match  
DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response.  
- `<DHCP-OPTION>` – Specify the DHCP option value. Devices matching the specified option value are redirected. |
| `fqdn` `<FQDN>` | Configures the FQDN to match  
FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain.  
- `<FQDN>` – Specify the FQDN. Devices matching the specified value are redirected. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip [<START-IP> <END-IP>] [<IP/MASK>] | Configures a range of IP addresses and subnet address. Devices having IPv4 addresses within the specified range or are part of the specified subnet are redirected.  
  - `<START-IP>` – Specify the first IPv4 address in the range.  
  - `<END-IP>` – Specify the last IPv4 address in the range.  
  - `<IP/MASK>` – Specify the IPv4 subnet and mask to match against the device’s IP address. |
| level[1|2] | Configures the routing level  
  - `level1` – Specifies level 1 as local routing  
  - `level2` – Specifies level2 as inter-site routing |
| ipv6 [<START-IP> <END-IP>] [<IP/MASK>] | Redirects if a device’s IPv6 address matches the specified IP address or is within the specified IP address range  
  - `<START-IP>` – Specify the first IPv6 address in the range.  
  - `<END-IP>` – Specify the last IPv6 address in the range.  
  - `<IP/MASK>` – Specify the IPv6 subnet and mask to match against the device’s IP address. |
| lldp-match <LLDP-STRING> | Configures the device location to match, based on LLDP snoop strings  
  LLDP is a vendor neutral link layer protocol used to advertise a network device’s identity, capabilities, and neighbors on a local area network.  
  - `<LLDP-STRING>` – Specify the location. Devices matching the specified string are redirected. |
| mac <START-MAC> {<END-MAC>} | Configures a single or a range of MAC addresses. Devices matching the specified values are redirected.  
  - `<START-MAC>` – Specify the first MAC address in the range. Provide only this MAC address to filter a single device.  
  - `<END-MAC>` – Optional. Specify the last MAC address in the range. |
| model-number <MODEL-NUMBER> | Configures the device model number  
  - `<MODEL-NUMBER>` – Specify the model number. Devices matching the specified model number are redirected. |
| pool <1-2> | Configures the controller pool  
  - `<1-2>` – Configures the pool to which the specified controller belongs to. The default pool value is 1. |
| serial-number <SERIAL-NUMBER> | Configures the device’s serial number  
  - `<SERIAL-NUMBER>` – Specify the serial number. Devices matching the specified serial number are redirected. |
| vlan <VLAN-ID> | Configures the VLAN ID  
  - `<VLAN-ID>` – Specify the VLAN ID. Devices assigned to the specified VLAN are redirected. |
| upgrade | Optional. Upgrades APs before redirecting the device for adoption within the system |
Examples
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 4
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 5
controller 192.168.13.10 model-number AP-8132-66040-US
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
  default-adoption
    adopt ap81xx precedence 1 profile default-ap81xx vlan 1
    deny ap71xx precedence 2 model-number AP7131N
    deny ap71xx precedence 3 ip 192.168.13.23 192.168.13.23
    redirect ap81xx precedence 5 controller 192.168.13.10 model-number AP-8132-66040-US
rfs4000-229D58(config-auto-provisioning-policy-test)#
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap621 precedence 1
controller host ip 192.168.13.4 192.168.13.8 upgrade
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
  redirect ap621 precedence 1 controller host ip 192.168.13.4 192.168.13.8 upgrade
rfs4000-229D58(config-auto-provisioning-policy-test)#

Related Commands

| no        | Removes a redirect rule |
## 9.1.6 upgrade

**auto-provisioning-policy**

Adds a device upgrade rule to this auto provisioning policy. When applied to a controller, the upgrade rule ensures adopted devices, of the specified type, are upgraded automatically.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```
upgrade [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7532|ap7552|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any
```

### Parameters

- **upgrade [anyap|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7532|ap7552|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx5500|nx65xx|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any**

- **any** Indicates any device. Any device, of the selected type, is upgraded. For example, if the device type selected is AP621, any AP621 device is upgraded.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>upgrade</strong></td>
<td>Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, VX9000, and NX9600 series.</td>
</tr>
<tr>
<td><strong>precedence</strong></td>
<td>Sets the rule precedence. Rules with lower values get precedence over rules with higher values.</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Indicates any device. Any device, of the selected type, is upgraded. For example, if the device type selected is AP621, any AP621 device is upgraded.</td>
</tr>
</tbody>
</table>

### redirect

Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.

The different device types are: anyap, AP621, AP622, AP650, AP651, AP652, AP6522, AP653, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX5500, NX65XX, NX75XX, NX9000, and VX9600 series.

**Note:** 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the type.

### precedence <1-10000>

Sets the rule precedence. Rules with lower values get precedence over rules with higher values.

### cdp-match <LOCATION-SUBSTRING>

Configures the device location to match, based on CDP snoop strings

- `<LOCATION-SUBSTRING>` – Specify the location. Devices matching the specified string are upgraded.

### dhcp-option <DHCP-OPTION>

Configures the DHCP options to match

DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response.

- `<DHCP-OPTION>` – Specify the DHCP option value. Devices matching the specified value are upgraded.

### fqdn <FQDN>

Configures the FQDN to match

FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain.

- `<FQDN>` – Specify the FQDN. Devices matching the specified value are upgraded.

### ip [<START-IP> <END-IP>|<IP/MASK>]

Configures a range of IP addresses and subnet address. Devices having IPv4 addresses within the specified range or are part of the specified subnet are upgraded.

- `<START-IP>` – Specify the first IPv4 address in the range.
- `<END-IP>` – Specify the last IPv4 address in the range.
- `<IP/MASK>` – Specify the IPv4 subnet and mask to match against the device’s IP address.

### ipv6 [<START-IP> <END-IP>|<IP/MASK>]

Upgrades if a device's IPv6 address matches the specified IP address or is within the specified IP address range

- `<START-IP>` – Specify the first IPv6 address in the range.
- `<END-IP>` – Specify the last IPv6 address in the range.
- `<IP/MASK>` – Specify the IPv6 subnet and mask to match against the device’s IP address.

### lldp-match <LLDP-STRING>

Configures the device location to match, based on LLDP snoop strings

LLDP is a vendor neutral link layer protocol used to advertise a network device’s identity, capabilities, and neighbors on a local area network.

- `<LLDP-STRING>` – Specify the location. Devices matching the specified string are upgraded.
### Examples

```bash
rfs4000-229D58(config-auto-provisioning-policy-test)#upgrade ap621 precedence 1 any
rfs4000-229D58(config-auto-provisioning-policy-test)#upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#show context auto-provisioning-policy test
    upgrade ap621 precedence 1 any
    upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an upgrade rule</td>
</tr>
</tbody>
</table>
9.1.7 \texttt{no}

\textit{auto-provisioning-policy}

Removes a deny, permit, or redirect rule from the specified auto provisioning policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

\textbf{Syntax}

\texttt{no \ [adopt|default-adoption|deny|evaluate-always|redirect|upgrade]}

\texttt{no adopt precedence \ <1-10000>}

\texttt{no deny precedence \ <1-10000>}

\texttt{no evaluate-always}

\texttt{no default-adoption}

\texttt{no redirect precedence \ <1-10000>}

\texttt{no upgrade precedence \ <1-10000>}

\textbf{Parameters}

- \texttt{no \ <PARAMETERS>}

\texttt{no \ <PARAMETERS>} Removes a deny, permit, or redirect rule from the specified auto provisioning policy

\textbf{Examples}

The following example shows the auto-provisioning-policy 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
  default-adoption
  adopt ap81xx precedence 1 profile default-ap81xx vlan 1
  deny ap71lx xx precedence 2 model-number AP7131N
  deny ap71lx xx precedence 3 ip 192.168.13.23 192.168.13.23
  redirect ap81xx precedence 5 controller 192.168.13.10 model-number AP-8132-66040-US
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

The following example shows the auto-provisioning-policy 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-auto-provisioning-policy-test)#no default-adoption
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 2
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 3
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 5
```

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
  upgrade ap621 precedence 1 any
  upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

```
rfs4000-229D58(config-auto-provisioning-policy-test)#no upgrade precedence 1
```

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
  upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```
This chapter summarizes the association ACL policy commands in the CLI command structure. An association ACL is a policy-based Access Control List (ACL) that either prevents or allows wireless clients from connecting to a controller managed WLAN.

System administrators can use an association ACL to grant or restrict wireless clients access to the WLAN by specifying client MAC addresses or range of MAC addresses to either include or exclude from controller connectivity. Association ACLs are applied to WLANs as an additional access control mechanism.

Use the (config) instance to configure the association ACL policy. To navigate to the association-acl-policy instance, use the following commands:

```
<DEVICE>(config)#association-acl-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#association-acl-policy test
rfs7000-37FABE(config-assoc-acl-test)#
```

Association ACL Mode commands:

- `deny` Specify MAC addresses to be denied
- `no` Negate a command or set its defaults
- `permit` Specify MAC addresses to be permitted
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-assoc-acl-test)#
```

**NOTE:** If creating a new association ACL policy, provide a name specific to its function. Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.
Before defining an association ACL policy and applying it to a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The name and configuration of an association ACL policy should meet the requirements of the WLANs it may map to. However, be careful not to name ACLs after specific WLANs, as individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a layer 2 interface. If a MAC ACL is already configured on a layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
10.1 association-acl-policy

The following table summarizes association ACL policy configuration commands:

Table 10.1 Association-ACL-Policy-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Specifies a range of MAC addresses denied access to the WLAN</td>
<td>page 10-4</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny or permit rule from this association ACL policy</td>
<td>page 10-6</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies a range of MAC addresses allowed access to the WLAN</td>
<td>page 10-7</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
10.1.1 deny

- association-acl-policy

Creates a list of devices denied access to the managed network. Devices are identified by their MAC address. A single MAC address or a range of MAC addresses can be denied access. This command also sets the precedence on how deny rules are applied. Up to a thousand (1000) deny rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

deny <STARTING-MAC> [ <ENDING-MAC> | precedence ]

deny <STARTING-MAC> precedence <1-1000>
deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

Parameters

- deny <STARTING-MAC> precedence <1-1000>
- To add a single device, enter its MAC address in the <STARTING-MAC> parameter.

- precedence <1-1000>
- Sets a precedence rule. Rules are applied in an increasing order of precedence.
  - <1-1000> – Specify a precedence value from 1 - 1000.

Usage Guidelines

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are applied in an increasing order of precedence. That means the rule with precedence 1 is applied first, then the rule with precedence 2 and so on.
Examples

rfs7000-37FABE(config-assoc-acl-test)#deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150

rfs7000-37FABE(config-assoc-acl-test)#deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160

rfs7000-37FABE(config-assoc-acl-test)#show context association-acl-policy test
   deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
   deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160
rfs7000-37FABE(config-assoc-acl-test)#

Related Commands

| no | Removes a deny rule based on its precedence value |
10.1.2 no

association-acl-policy

Removes a deny or permit rule from this association ACL policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|permit]

no deny <STARTING-MAC> precedence <1-1000>
no deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

no permit <STARTING-MAC> precedence <1-1000>
no permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

Parameters

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes a deny or permit rule from this association ACL policy</th>
</tr>
</thead>
</table>

Examples

The following example shows the association ACL policy ‘test’ settings before the ‘no’ commands is executed:

rfs7000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
  deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
rfs7000-37FABE(config-assoc-acl-test)#

rfs7000-37FABE(config-assoc-acl-test)#no deny 11-22-33-44-56-01 11-22-33-44-56-FF precedence 160

The following example shows the association ACL policy ‘test’ settings after the ‘no’ commands is executed:

rfs7000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
  deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
rfs7000-37FABE(config-assoc-acl-test)#
### 10.1.3 permit

`association-acl-policy`

Creates a list of devices allowed access to the managed network. Devices are permitted access based on their MAC address. A single MAC address or a range of MAC addresses can be specified. This command also sets the precedence on how permit list rules are applied. Up to a thousand (1000) permit rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

**Supported in the following platforms:**
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

- `permit <STARTING-MAC> [ <ENDING-MAC>|precedence ]`
- `permit <STARTING-MAC> precedence <1-1000>`
- `permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>`

**Parameters**

- `permit <STARTING-MAC>`: adds a single device or a set of devices to the permit list. To add a single device, enter its MAC address in the `<STARTING-MAC>` parameter.
- `precedence <1-1000>`: specifies a rule precedence. Rules are applied in an increasing order of precedence.
  - `<1-1000>` – Specify a value from 1 - 1000.
- `permit <STARTING-MAC> <ENDING-MAC>`: adds a single device or a set of devices to the permit list. To add a set of devices, provide the MAC address range.

**Usage Guidelines**

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are applied to packets in an increasing order of precedence. That means the rule with precedence 1 is applied first, then the rule with precedence 2 and so on.
Examples

rfs7000-37FABE(config-assoc-acl-test)# permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170

rfs7000-37FABE(config-assoc-acl-test)# permit 11-22-33-44-67-01 precedence 180

rfs7000-37FABE(config-assoc-acl-test)# show context association-acl-policy test
deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170
permit 11-22-33-44-67-01 11-22-33-44-67-01 precedence 180

rfs7000-37FABE(config-assoc-acl-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes a permit rule based on its precedence</td>
</tr>
</tbody>
</table>
This chapter summarizes IPv4, IPv6, and MAC access list commands in the CLI command structure. Access lists control access to the managed network using a set of rules also known as Access Control Entries (ACEs). Each rule specifies an action taken when a packet matches that rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. A set of deny and/or permit rules based on IP (IPv4 and IPv6) addresses constitutes a IP Access Control List (ACL). Similarly, a set of deny and/or permit rules based on MAC addresses constitutes a MAC ACL.

Within a managed network, IP ACLs (IPv4 and IPv6) are used as firewalls to filter packets, and may also mark packets, based on the IP address which they arrive, as opposed to filtering packets on layer 2 ports. IP based firewall rules are specific to the source and destination IP addresses and have unique precedence orders assigned. Both IP and non-IP traffic on the same layer 2 or port interface can be filtered by applying an IP ACL. With either IPv4 or IPv6, create access rules for traffic entering a controller, service platform, or access point interface, because if you are going to deny specific types of packets, it’s recommended you do it before the controller, service platform, or access point spends time processing them, since access rules are given priority over other types of firewall rules.

IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

MAC ACLs are firewalls that filter or mark packets based on the MAC address which they arrive, as opposed to filtering packets on layer 2 ports. Optionally filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to controller managed packet traffic.

Once defined, a IP and/or MAC ACL (consisting of a set of firewall rules) must be applied to an interface to be a functional filtering tool.

Firewall supported devices (access points, wireless controllers, and service platforms) process firewall rules (within an IP/MAC ACL) sequentially, in ascending order of their precedence value. When a packet (network traffic) matches a rule, the firewall applies the action specified in the rule to determine whether the traffic is allowed or denied. Once a match is made, the firewall does not process subsequent rules in the ACL.

The WiNG software enables the configuration of IP SNMP ACLs. These ACLs control access by combining IP ACLs with SNMP server community strings.

The following ACLs are supported:

- **ip-access-list**
- **mac-access-list**
- **ipv6-access-list**
- **ip-snmp-access-list**
- **ex3500-ext-access-list**
• **ex3500-std-access-list**

Use IP and MAC commands under the global configuration to create an access list.

• When the access list is applied on an Ethernet port, it becomes a port ACL.
• When the access list is applied on a VLAN interface, it becomes a router ACL.

Use the (config) instance to configure a new ACL or modify an existing ACL. To navigate to the (config-access-list) instance, use the following commands:

```
<DEVICE>(config)#ip access-list <IP-ACCESS-LIST-NAME>
<DEVICE>(config)#mac access-list <MAC-ACCESS-LIST-NAME>
<DEVICE>(config)#ipv6 access-list <IPv6-ACCESS-LIST-NAME>
<DEVICE>(config)#ip snmp-access-list <SNMP-ACCESS-LIST-NAME>
<DEVICE>(config)#ex3500-ext-access-list <EX3500-EXT-ACCESS-LIST-NAME>
<DEVICE>(config)#ex3500-std-access-list <EX3500-STD-ACCESS-LIST-NAME>
```

**NOTE:** If creating an new ACL policy, provide a name that uniquely identifies its purpose. The name cannot exceed 32 characters.

---

**ip-access-list**

```
rfs7000-37FABE(config)#ip access-list test
rfs7000-37FABE(config-ip-acl-test)#?
```

ACL Configuration commands:

- `deny` Specify packets to reject
- `disable` Disable rule if not needed
- `insert` Insert this rule (instead of overwriting a existing rule)
- `no` Negate a command or set its defaults
- `permit` Specify packets to forward

```
clrscr  Clears the display screen  
commit  Commit all changes made in this session  
do  Run commands from Exec mode  
end  End current mode and change to EXEC mode  
ext  End current mode and down to previous mode  
help  Description of the interactive help system  
revert  Revert changes  
service  Service Commands  
show  Show running system information  
write  Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-ip-acl-test)#
```

---

**mac-access-list**

```
rfs7000-37FABE(config)#mac access-list test
rfs7000-37FABE(config-mac-acl-test)#?
```

MAC Extended ACL Configuration commands:

- `deny` Specify packets to reject
- `disable` Disable rule if not needed
- `ex3500` EX3500 device
- `insert` Insert this rule (instead of overwriting a existing rule)
- `no` Negate a command or set its defaults
- `permit` Specify packets to forward

```
clrscr  Clears the display screen  
do  Run commands from Exec mode  
commit  Commit all changes made in this session  
end  End current mode and change to EXEC mode
```

```
rfs7000-37FABE(config-mac-acl-test)#
```
exit     End current mode and down to previous mode
help     Description of the interactive help system
revert   Revert changes
service  Service Commands
show     Show running system information
write    Write running configuration to memory or terminal

rfs7000-37FABE(config-mac-acl-test)#

**ipv6-access-list**

rfs7000-37FABE(config-ipv6-acl-test)#
IPv6 Access Control Mode commands:
deny     Specify packets to reject
no       Negate a command or set its defaults
permit   Specify packets to forward
clrscr   Clears the display screen
commit   Commit all changes made in this session
do      Run commands from Exec mode
end      End current mode and change to EXEC mode
exit     End current mode and down to previous mode
help     Description of the interactive help system
revert   Revert changes
service  Service Commands
show     Show running system information
write    Write running configuration to memory or terminal

rfs7000-37FABE(config-ipv6-acl-test)#

**ip-snmp-access-list**

nx9500-6C8809(config-ip-snmp-acl-test)#
SNMP ACL Configuration commands:
deny     Specify packets to reject
no       Negate a command or set its defaults
permit   Specify packets to forward
clrscr   Clears the display screen
commit   Commit all changes made in this session
do      Run commands from Exec mode
end      End current mode and change to EXEC mode
exit     End current mode and down to previous mode
help     Description of the interactive help system
revert   Revert changes
service  Service Commands
show     Show running system information
write    Write running configuration to memory or terminal

nx9500-6C8809(config-ip-snmp-acl-test)#
The WiNG NOC controller also has the capabilities of adopting and managing EX3500 series switch. These switches are Gigabit Ethernet layer 2 switches with either 24 or 48 10/100/1000-BASE-T ports, and four Small Form Factor Pluggable (SFP) transceiver slots for fiber connectivity. Once adopted to the NOC, various ACLs specifically defined for a EX3500 switch can be used to either prevent or allow specific clients from using it.
The following EX3500 ACLs are supported:
- ex3500-ext-access-list
- ex3500-std-access-list
- **ex3500**: This configures a EX3500 deny or permit rule in a MAC ACL.

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
11.1 ip-access-list

The following table summarizes IP access list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined for specified address(es).</td>
<td>page 11-5</td>
</tr>
<tr>
<td>disable</td>
<td>Disables an existing deny or permit rule without removing it from the ACL</td>
<td>page 11-16</td>
</tr>
<tr>
<td>insert</td>
<td>Inserts a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence</td>
<td>page 11-19</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny and/or a permit access rule from a IP ACL</td>
<td>page 11-21</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined for specified address(es).</td>
<td>page 11-22</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
11.1.1 deny

`ip-access-list`

Creates a deny rule that rejects packets from a specified source IP and/or to a specified destination IP. You can also use this command to modify an existing deny rule.

NOTE: Use a decimal value representation to implement a permit/deny designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

deny [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]

deny <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID]|<SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-HOST-IP>] [<NETWORK-GROUP-ALIAS-NAME>] [log,mark [8021p <0-7>|dscp <0-63>],

rule-precedence <1-5000>) {rule-description <LINE>

deny dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>)

{rule-description <LINE>}

deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>]

host <SOURCE-HOST-IP> [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>)

{rule-description <LINE>}

deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>]

host <SOURCE-HOST-IP> [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {rule-description <LINE>}

deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]

[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>]

host <SOURCE-HOST-IP> [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {rule-description <LINE>}

deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>]

host <SOURCE-HOST-IP> [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq <SOURCE-PORT>]

host <DEST-HOST-IP> [range <START-PORT> <END-PORT>] [eq [1-65535]|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|ntlm|ntpd|pop3|smtp|ssh|telnet|tftp|www] [range <START-PORT> <END-PORT>]

(log,rule-precedence <1-5000>) {rule-description <LINE>}

```
### Parameters

- **deny** `<NETWORK-SERVICE-ALIAS-NAME>` [ `<SOURCE-IP/MASK>` | `<NETWORK-GROUP-ALIAS-NAME>` | `any` ] from-vlan `<VLAN-ID>` | host `<SOURCE-HOST-IP>` ] [ `<DEST-IP/MASK>` | `any` ] host `<DEST-HOST-IP>` `<NETWORK-GROUP-ALIAS-NAME>` ] { (log, mark [ 8021p < 0-7> | dscp < 0-63> ], rule-precedence < 1-5000> ) } { (rule-description < LINE> ) }

| `<NETWORK-SERVICE-ALIAS-NAME>` | Applies this deny rule to packets based on service protocols and ports specified in the network-service alias  
|----------------------------------|-------------------------------------------------------------  
|                                  | • `<NETWORK-SERVICE-ALIAS-NAME>` – Specify the network-service alias name (should be existing and configured).  
|                                  | A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL deny rule.  
|                                  | **Note:** For more information on configuring network-service alias, see alias.  
| `<SOURCE-IP/MASK>` | Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are dropped.  
| `<NETWORK-GROUP-ALIAS-NAME>` | Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are dropped.  
|                                  | • `<NETWORK-GROUP-ALIAS-NAME>` – Specify the network-group alias name (should be existing and configured).  
|                                  | A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).  
| `any` | Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are dropped.  
| `from-vlan` `<VLAN-ID>` | Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are dropped.  
|                                  | • `<VLAN-ID>` – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).  
|                                  | **Note:** Use this option with WLANs and port ACLs.  
| `host` `<SOURCE-HOST-IP>` | Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped.  
|                                  | • `<SOURCE-HOST-IP>` – Specify the source host’s exact IP address in the A.B.C.D format.  
| `<DEST-IP/MASK>` | Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are dropped.  
| `any` | Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are dropped.  
| `host` `<DEST-HOST-IP>` | Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are dropped.  
|                                  | • `<DEST-HOST-IP>` – Specify the destination host’s exact IP address in the A.B.C.D format.  

| **<NETWORK-GROUP-ALIAS-NAME>** | Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are dropped.  
• **<NETWORK-GROUP-ALIAS-NAME>** – Specify the network-group alias name (should be existing and configured). |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>log</strong></td>
<td>Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</td>
</tr>
</tbody>
</table>
| **mark [8021p <0-7>|dscp <0-63>]** | Specifies packets to mark  
• 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority  
• dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header |
| **rule-precedence <1-5000>** | The following keywords are recursive and common to all of the above parameters:  
• rule-precedence – Assigns a precedence for this deny rule  
• <1-5000> – Specify a value from 1 - 5000.  
**Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.  
• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |
| **deny dns-name [contains|exact|suffix] <WORD>** | Applies this deny rule to packets based on dns-names specified in the network-service  
**{(rule-description <LINE>)}** |
| **dns-name** | Applies this deny rule to packets based on dns-names specified in the network-service  
**{(rule-description <LINE>)}** |
| **contains** | Matches any hostname which has this DNS label. (for example *.test.*) |
| **exact** | Matches an exact hostname as specified in the network-service |
| **suffix** | Matches any hostname as suffix (for example *.test) |
| **<WORD>** | Identifies a specific host (as the source to match) by its domain name. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped. |
| **log** | Logs all deny events matching this dns entry. If a dns-name is matched an event is logged. |
| **rule-precedence <1-5000>** | The following keywords are recursive and common to all of the above parameters:  
• rule-precedence – Assigns a precedence for this deny rule  
• <1-5000> – Specify a value from 1 - 5000.  
**Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.  
• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |
| **deny icmp [<SOURCE-IP/MAK<1-5000>)] | Applies this deny rule to Internet Control Message Protocol (ICMP) packets only  
**{(rule-description <LINE>)}** |
| **<SOURCE-IP/MAK** | Applies this deny rule to Internet Control Message Protocol (ICMP) packets only  
**{(rule-description <LINE>)}** |
<p>| <strong>&lt;NETWORK-GROUP-NAME&gt;</strong> | Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are dropped. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<NETWORK-GROUP-ALIAS-NAME>` | Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are dropped.  
  - `<NETWORK-GROUP-ALIAS-NAME>` – Specify the network-group alias name (should be existing and configured). |
| `any`                     | Specifies the source as any IP address. ICMP packets received from any source are dropped.       |
| `from-vlan` `<VLAN-ID>`    | Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are dropped.  
  - `<VLAN-ID>` – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). |
| `host` `<SOURCE-HOST-IP>`  | Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are dropped.  
  - `<SOURCE-HOST-IP>` – Specify the source host’s exact IP address in the A.B.C.D format. |
| `<DEST-IP/MASK>`           | Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are dropped. |
| `<NETWORK-GROUP-ALIAS-NAME>` | Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are dropped.  
  - `<NETWORK-GROUP-ALIAS-NAME>` – Specify the network-group alias name (should be existing and configured). |
| `any`                     | Specifies the destination as any IP address. ICMP packets addressed to any destination are dropped. |
| `host` `<DEST-HOST-IP>`    | Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are dropped.  
  - `<DEST-HOST-IP>` – Specify the destination host’s exact IP address in the A.B.C.D format. |
| `<ICMP-TYPE>`              | Defines the ICMP packet type  
  For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO. |
| `<ICMP-CODE>`              | Defines the ICMP message type  
  For example, an ICMP code 3 indicates “Destination Unreachable”, code 1 indicates “Host Unreachable”, and code 3 indicates “Port Unreachable.”  
  **Note:** After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match. |
| `log`                      | Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e., a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged. |
| `rule-precedence` `<1-5000>` | The following keywords are recursive and common to all of the above parameters:  
  - `rule-precedence` – Assigns a precedence for this deny rule  
  - `<1-5000>` – Specify a value from 1 - 5000.  
  - `rule-description` – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |
• deny ip [<SOURCE-IP/MASK> | <NETWORK-GROUP-ALIAS-NAME> | any | from-vlan <VLAN-ID> | host <SOURCE-HOST-IP>] [<DEST-IP/MASK> | <NETWORK-GROUP-ALIAS-NAME> | any | host <DEST-HOST-IP>] (log, rule-precedence <1-5000>) { (rule-description <LINE>)

<table>
<thead>
<tr>
<th>ip</th>
<th>Applies this deny rule to IP packets only</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SOURCE-IP/MASK&gt;</td>
<td>Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are dropped.</td>
</tr>
</tbody>
</table>
| <NETWORK-GROUP-ALIAS-NAME> | Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are dropped. 
  • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). |
| any | Specifies the source as any IP address. IP packets received from any source are dropped. |
| from-vlan <VLAN-ID> | Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are dropped. 
  • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). 
  **Note:** Use this option with WLANs and port ACLs. |
| host <SOURCE-HOST-IP> | Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are dropped. 
  • <SOURCE-HOST-IP> – Specify the source host’s exact IP address in the A.B.C.D format. |
| <DEST-IP/MASK> | Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are dropped. |
| any | Specifies the destination as any IP address. IP packets addressed to any destination are dropped. |
| host <DEST-HOST-IP> | Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are dropped. 
  • <DEST-HOST-IP> – Specify the destination host’s exact IP address in the A.B.C.D format. |
| <NETWORK-GROUP-ALIAS-NAME> | Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are dropped. 
  • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). |
| log | Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged. |
| rule-precedence <1-5000> rule-description <LINE> | The following keywords are recursive and common to all of the above parameters: 
  • rule-precedence – Assigns a precedence for this deny rule 
  • <1-5000> – Specify a value from 1 - 5000. 
  **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. 
  • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |

<table>
<thead>
<tr>
<th><strong>proto</strong></th>
<th>Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter</th>
</tr>
</thead>
</table>
| `<PROTOCOL-NUMBER>` | Filters protocols using their Internet Assigned Numbers Authority (IANA) protocol number  
- `<PROTOCOL-NUMBER>` – Specify the protocol number. |
| `<PROTOCOL-NAME>` | Filters protocols using their IANA protocol name  
- `<PROTOCOL-NAME>` – Specify the protocol name. |
| **eigrp** | Identifies the Enhanced Internet Gateway Routing Protocol (EIGRP) protocol (number 88)  
EIGRP enables routers to maintain copies of neighbors’ routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables. |
| **gre** | Identifies the General Routing Encapsulation (GRE) protocol (number 47)  
GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination. |
| **igmp** | Identifies the Internet Group Management Protocol (IGMP) protocol (number 2)  
IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them. |
| **igp** | Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9)  
IGP enables exchange of information between hosts and routers within a managed network. The most commonly used interior gateway protocol (IGP) protocols are: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) |
| **ospf** | Identifies the OSPF protocol (number 89)  
OSPF is a link-state interior gateway protocol (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. |
| **vrrp** | Identifies the Virtual Router Redundancy Protocol (VRRP) protocol (number 112)  
VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;SOURCE-IP/MASK&gt;</code></td>
<td>Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are dropped.</td>
</tr>
</tbody>
</table>
| `<NETWORK-GROUP-Alias-NAME>` | Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are dropped.  
  - `<NETWORK-GROUP-Alias-NAME>` – Specify the network-group alias name (should be existing and configured). |
| any | Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped. |
| from-vlan <VLAN-ID> | Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are dropped.  
  - `<VLAN-ID>` – Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20). |
| host `<SOURCE-HOST-IP>` | Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped.  
  - `<SOURCE-HOST-IP>` – Specify the source host’s exact IP address in the A.B.C.D format. |
| `<DEST-IP/MASK>` | Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are dropped. |
| any | Specifies the destination as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped. |
| host `<DEST-HOST-IP>` | Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are dropped.  
  - `<SOURCE-HOST-IP>` – Specify the destination host’s exact IP address in the A.B.C.D format. |
| `<NETWORK-GROUP-Alias-NAME>` | Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are dropped.  
  - `<NETWORK-GROUP-Alias-NAME>` – Specify the network-group alias name (should be existing and configured). |
| Note: | After specifying the source and destination IP address(es), specify the action taken in case of a match. |
| log | Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged. |
| rule-precedence `<1-5000>` | The following keywords are recursive and common to all of the above parameters:  
  - rule-precedence – Assigns a precedence for this deny rule  
  - `<1-5000>` – Specify a value from 1 - 5000. |
| rule-description `<LINE>` | Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.  
  - rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |
**deny** [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>| [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] eq <SOURCE-PORT>|host <DEST-HOST-IP>| range <START-PORT> <END-PORT>| (log,rule-precedence <1-5000>){(rule-description <LINE>)}

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Applies this deny rule to TCP packets only</td>
</tr>
<tr>
<td>udp</td>
<td>Applies this deny rule to UDP packets only</td>
</tr>
<tr>
<td>&lt;SOURCE-IP/MASK&gt;</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are dropped.</td>
</tr>
<tr>
<td>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are dropped.</td>
</tr>
<tr>
<td>any</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the source as any IP address. TCP/UDP packets received from any source are dropped.</td>
</tr>
<tr>
<td>from-vlan &lt;VLAN-ID&gt;</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are dropped.</td>
</tr>
<tr>
<td>host &lt;SOURCE-HOST-IP&gt;</td>
<td>Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are dropped.</td>
</tr>
<tr>
<td>&lt;DEST-IP/MASK&gt;</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are dropped.</td>
</tr>
<tr>
<td>any</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the destination as any IP address. TCP/UDP packets received from any destination are dropped.</td>
</tr>
<tr>
<td>eq &lt;SOURCE-PORT&gt;</td>
<td>Identifies a specific source port</td>
</tr>
<tr>
<td>host &lt;DEST-HOST-IP&gt;</td>
<td>Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are dropped.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code></td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are dropped. • <code>&lt;NETWORK-ALIAS-GROUP-NAME&gt;</code> – Specify the network-group alias name (should be existing and configured).</td>
</tr>
<tr>
<td><strong>range</strong></td>
<td>Specifies a range of source ports • <code>&lt;START-PORT&gt;</code> – Specify the first port in the range. • <code>&lt;END-PORT&gt;</code> – Specify the last port in the range.</td>
</tr>
<tr>
<td><strong>eq</strong></td>
<td>Identifies a specific destination or protocol port to match • <code>&lt;1-65535&gt;</code> – The destination port is designated by its number • <code>&lt;SERVICE-NAME&gt;</code> – Specifies the service name • bgp – The designated Border Gateway Protocol (BGP) protocol port (179) • dns – The designated Domain Name System (DNS) protocol port (53) • ftp – The designated File Transfer Protocol (FTP) protocol port (21) • ftp-data – The designated FTP data port (20) • gopher – The designated GROPER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated Lightweight Directory Access Protocol (LDAP) protocol port (389) • nntp – The designated Network News Transfer Protocol (NNTP) protocol port (119) • ntp – The designated Network Time Protocol (NTP) protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated Session Initiation Protocol (SIP) protocol port (5060) • smtp – The designated Simple Mail Transfer Protocol (SMTP) protocol port (25) • ssh – The designated Secure Shell (SSH) protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated Trivial File Transfer Protocol (TFTP) protocol port (69) • www – The designated www protocol port (80)</td>
</tr>
<tr>
<td><strong>range</strong></td>
<td>Specifies a range of destination ports • <code>&lt;START-PORT&gt;</code> – Specify the first port in the range. • <code>&lt;END-PORT&gt;</code> – Specify the last port in the range.</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>Logs all deny events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</td>
</tr>
<tr>
<td><strong>rule-precedence</strong></td>
<td>The following keywords are recursive and common to all of the above: • rule-precedence – Assigns a precedence for this deny rule • <code>&lt;1-5000&gt;</code> – Specify a value from 1 - 5000. <strong>Note</strong>: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</td>
</tr>
</tbody>
</table>
Usage Guidelines
Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- IP
- ICMP
- TCP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last access control entry (ACE) in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria
- Select ICMP as the protocol to allow or deny ICMP packets. Selecting ICMP filters ICMP packets based on ICMP type and code.

Examples
rfs7000-37FABE(config-ip-acl-test)#deny proto vrrp any any log rule-precedence 600
rfs7000-37FABE(config-ip-acl-test)#deny proto ospf any any log rule-precedence 650
rfs7000-6DCD4B(config-ip-acl-acl)#deny dns-name contains rfs7000 log rule-precedence 1
rfs7000-6DCD4B(config-ip-acl-acl)#show context
  ip access-list acl
deny dns-name contains rfs7000 log rule-precedence 1
rfs7000-6DCD4B(config-ip-acl-acl)#

rfs7000-37FABE(config-ip-acl-test)#show context
  ip access-list test
deny proto vrrp any any log rule-precedence 600
deny proto ospf any any log rule-precedence 650
rfs7000-37FABE(config-ip-acl-test)#

Using aliases in IP access list.
The following examples show the usage of network-group aliases:
rfs4000-229D58(config)#ip access-list bar
Example 1:
rfs4000-229D58(config-ip-acl-bar)#permit ip $foo any rule-precedence 10
Example 2
rfs4000-229D58(config-ip-acl-bar)#permit tcp 192.168.100.0/24 $foobar eq ftp rule-precedence 20
Example 3
rfs4000-229D58(config-ip-acl-bar)#deny ip $guest $lab rule-precedence 30
  In example 1, network-group alias $foo is used as a source
  In example 2, network-group alias $foobar is used as a destination
  In example 3, network-group aliases $guest and $lab are used as source and destination respectively.

The following examples show the usage of network-service aliases:
Example 4

rfs4000-229D58(config-ip-acl-bar)# permit $kerberos 10.60.20.0/24 $kerberos-servers log rule-precedence 40

Example 5

rfs4000-229D58(config-ip-acl-bar)#permit $Tandem 10.60.20.0/24 $Tandem-servers log rule-precedence 50

In examples 4, and 5:

• The network-service aliases ($kerberos and $Tandem) define the destination protocol-port combinations
• The source network is 10.60.20.0/24
• The destination network-address combinations are defined by the network-group aliases ($kerberos-servers and $Tandem-servers)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes a specified IP deny access rule</td>
</tr>
<tr>
<td>alias</td>
<td>Creates and configures aliases (network, VLAN, and service)</td>
</tr>
</tbody>
</table>
### 11.1.2 disable

**ip-access-list**

Disables an existing deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9600

**Syntax**

```plaintext
disable [deny|insert|permit]  
disable [deny|insert [deny|permit] [permit] [NETWORK-SERVICE-ALIAS-NAME]|dns-name|icmp|ip|proto|tcp|udp]  
disable [deny|insert [deny|permit] [permit] [NETWORK-SERVICE-ALIAS-NAME]|dns-name [contains|exact|suffix] [icmp|ip|proto <PROTOCOL-OPTIONS>|tcp|udp]  
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [DEST-IP/MASK]<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence)
```

**Parameters**

- `disabled [deny|insert [deny|permit] [permit] [NETWORK-SERVICE-ALIAS-NAME]|dns-name [contains|exact|suffix] [icmp|ip|proto <PROTOCOL-OPTIONS>|tcp|udp] [SOURCE-IP/MASK]|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [DEST-IP/MASK]<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable [deny</td>
<td>insert [deny</td>
</tr>
<tr>
<td>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</td>
<td>Specifies the network-service alias, identified by the &lt;NETWORK-SERVICE-ALIAS-NAME&gt; keyword, associated with the deny/permit rule</td>
</tr>
<tr>
<td>dns-name [contains</td>
<td>exact</td>
</tr>
<tr>
<td>icmp</td>
<td>Disables a rule applicable to ICMP packets only</td>
</tr>
<tr>
<td>ip</td>
<td>Disables a rule applicable to IP packets only</td>
</tr>
<tr>
<td>proto &lt;PROTOCOL-OPTIONS&gt;</td>
<td>Disables a rule applicable to any Internet protocol other than TCP, UDP, or ICMP packets. <strong>Note:</strong> After specifying the packet type, specify the source and destination devices and network address(es) to match.</td>
</tr>
<tr>
<td>tcp</td>
<td>Disables a rule applicable to TCP packets only</td>
</tr>
<tr>
<td>udp</td>
<td>Disables a rule applicable to UDP packets only</td>
</tr>
</tbody>
</table>
The following example shows the ‘auto-tunnel-acl’ settings before the disable command is executed:

```
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#
```

```
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#disable permit ip host 200.200.200.99 any rule-precedence 3
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#
```

The following example shows the ‘auto-tunnel-acl’ settings after the disable command is executed:

```
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
disable permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#
```

```
rfs4000-229D58(config-ip-acl-test)#deny icmp any any log rule-precedence 1
```
In the following example a disable deny rule has been inserted in the IP ACL “test”:

```
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#
rfs4000-229D58(config-ip-acl-test)#disable insert deny ip any any log rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
disable deny ip any any log rule-precedence 2
permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Enables a disabled deny or permit rule</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Creates a new deny access rule or modifies an existing rule</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Creates a new permit access rule or modifies an existing rule</td>
</tr>
<tr>
<td><code>alias</code></td>
<td>Creates and configures a aliases (network, VLAN, and service)</td>
</tr>
</tbody>
</table>
**11.1.3 insert**

*ip-access-list*

Enables the insertion of a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence.

The insert option allows a new rule to be inserted within a IP access list. Consider an IP ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule's precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.

---

**NOTE:** NOT using `insert` when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

---

**Supported in the following platforms:**

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>], rule-precedence <1-5000>) {rule-description <LINE>}
```

**Parameters**

- `deny|permit` inserts a deny or a permit rule within an IP ACL.
- `<PARAMETERS>` provides the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here.
  - For more information on the deny rule, see `deny`.
  - For more information on the permit rule, see `permit`.
- `log` specifies the action taken for filtered packets.
  - Logs all deny/permit events matching this entry. If a source and/or destination IP address is matched an event is logged.
- `mark [8021p <0-7>|dscp <0-63>]` specifies packets to mark.
  - `8021p <0-7>` marks packets by modifying 802.1p VLAN user priority.
  - `dscp <0-63>` marks packets by modifying DSCP TOS bits in the header.
- `rule-precedence <1-5000>` assigns a precedence for this deny/permit rule.
  - `<1-5000>` specifies a value from 1 - 5000.
  - **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
  - `rule-description <LINE>` provides an optional description for the rule. Provide a description that uniquely identifies the purpose of the rule (should not exceed 128 characters in length).
NOTE: The log option is functional only for router ACL’s. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Examples
rfs4000-229D58(config-ip-acl-test)#deny tcp from-vlan 1 any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#

In the following example a new rule is inserted between the rules having precedences 1 and 2. The precedence of the existing precedence ‘2’ rule changes to precedence 3.

rfs4000-229D58(config-ip-acl-test)#insert deny ip any any rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
deny ip any any rule-precedence 2
permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#

Related Commands

| alias | Creates and configures aliases (network, VLAN, and service) |
11.1.4 no

- ip-access-list

Removes a deny, permit, or disable rule

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|disable|permit]

no [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp] <RULE-PARAMETERS>

no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp] <RULE-PARAMETERS>

Parameters
- no <PARAMETERS>
- no <PARAMETERS> Removes a deny, permit, or disable rule

Usage Guidelines

Removes an access list control entry. Provide the rule-precedence value when using the no command.

Examples

The following example shows the ACL 'test' settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
   deny proto vrrp any any log rule-precedence 600
   deny proto ospf any any log rule-precedence 650
rfs7000-37FABE(config-ip-acl-test)#
```

```
rfs7000-37FABE(config-ip-acl-test)#no deny proto vrrp any any rule-precedence 600
rfs7000-37FABE(config-ip-acl-test)#no deny proto ospf any any rule-precedence 650
```

The following example shows the ACL 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-ip-acl-test)#show context
ip access-list test
rfs7000-37FABE(config-ip-acl-test)#
```
11.1.5 permit

ip-access-list

Creates a permit rule that marks packets (from a specified source IP and/or to a specified destination IP) for forwarding. You can also use this command to modify an existing permit rule.

NOTE: Use a decimal value representation to implement a permit/deny designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
permit <NETWORK-SERVICE-ALIAS-NAME> [dns-name] [icmp] [ip] [proto] [tcp] [udp]
```

```
permit <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [from-vlan <VLAN-ID>] [host <SOURCE-HOST-IP>] [destination <DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [host <DEST-HOST-IP>] [log,mark [8021p <0-7>|dscp <0-63>], rule-precedence <1-5000>)] {(rule-description <LINE>)}
```

```
permit dns-name [contains] [exact] [suffix] <WORD> (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

```
permit dns-name exact <WORD> (log,mark [8021p <0-7>|dscp <0-63>], rule-precedence <1-5000>) {(rule-description <LINE>)}
```

```
permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [from-vlan <VLAN-ID>] [host <SOURCE-HOST-IP>] [destination <DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [host <DEST-HOST-IP>] [log,rule-precedence <1-5000>] {(rule-description <LINE>)}
```

```
permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [from-vlan <VLAN-ID>] [host <SOURCE-HOST-IP>] [destination <DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [host <DEST-HOST-IP>] [log,rule-precedence <1-5000>] {(rule-description <LINE>)}
```

```
permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [from-vlan <VLAN-ID>] [host <SOURCE-HOST-IP>] [destination <DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [host <DEST-HOST-IP>] [log,rule-precedence <1-5000>] {(rule-description <LINE>)}
```

```
permit [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [from-vlan <VLAN-ID>] [host <SOURCE-HOST-IP>] [destination <DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any] [eq <SOURCE-PORT>|host <DEST-HOST-IP>] [range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|smtp|smtp|ssh|telnet|tftp|www] [range <START-PORT> <END-PORT>] [log,rule-precedence <1-5000>] {(rule-description <LINE>)}
```

```
### Parameters

- **permit** `<NETWORK-SERVICE-ALIAS-NAME>` [ `<SOURCE-IP/MASK>` | `<NETWORK-GROUP-ALIAS-NAME>` | `any` ] [ from-vlan `<VLAN-ID>` | host `<SOURCE-HOST-IP>` ] [ `<DEST-IP/MASK>` | `any` | host `<DEST-HOST-IP>` ] `<NETWORK-GROUP-ALIAS-NAME>` [ (log, mark [8021p <0-7> | dscp <0-63>], rule-precedence <1-5000>) ] { (rule-description `<LINE>` ) }

| `<NETWORK-SERVICE-ALIAS-NAME>` | Applies this permit rule to packets based on service protocols and ports specified in the network-service alias  
| | • `<NETWORK-SERVICE-ALIAS-NAME>` – Specify the network-service alias name (should be existing and configured).  
| | A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL permit rule.  
| | **Note:** For more information on configuring network-service alias, see *alias*. |

| `<SOURCE-IP/MASK>` | Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are permitted. |

| `<NETWORK-GROUP-ALIAS-NAME>` | Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are permitted.  
| | • `<NETWORK-GROUP-ALIAS-NAME>` – Specify the network-group alias name (should be existing and configured).  
| | A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny). |

| `any` | Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are permitted. |

| from-vlan `<VLAN-ID>` | Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are permitted.  
| | • `<VLAN-ID>` – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).  
| | **Note:** Use this option with WLANs and port ACLs. |

| host `<SOURCE-HOST-IP>` | Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are permitted.  
| | • `<SOURCE-HOST-IP>` – Specify the source host’s exact IP address in the A.B.C.D format. |

| `<DEST-IP/MASK>` | Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are permitted. |

| `any` | Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are permitted. |

| host `<DEST-HOST-IP>` | Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are permitted.  
<p>| | • <code>&lt;DEST-HOST-IP&gt;</code> – Specify the destination host’s exact IP address in the A.B.C.D format. |</p>
<table>
<thead>
<tr>
<th>Permit DNS-Name Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are permitted.</td>
</tr>
<tr>
<td>• &lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>Specify the network-group alias name (should be existing and configured).</td>
</tr>
<tr>
<td>log</td>
<td>Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</td>
</tr>
<tr>
<td>mark [8021p &lt;0-7&gt;</td>
<td>dscp &lt;0-63&gt;]</td>
</tr>
<tr>
<td>• 8021p &lt;0-7&gt;</td>
<td>Marks packets by modifying 802.1.p VLAN user priority</td>
</tr>
<tr>
<td>• dscp &lt;0-63&gt;</td>
<td>Marks packets by modifying DSCP TOS bits in the header</td>
</tr>
<tr>
<td>rule-precedence &lt;1-5000&gt;</td>
<td>The following keywords are recursive and common to all of the above parameters:</td>
</tr>
<tr>
<td>• rule-precedence</td>
<td>Assigns a precedence for this permit rule</td>
</tr>
<tr>
<td>• &lt;1-5000&gt;</td>
<td>Specify a value from 1 - 5000.</td>
</tr>
<tr>
<td>Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</td>
<td></td>
</tr>
<tr>
<td>• rule-description</td>
<td>Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</td>
</tr>
<tr>
<td>• permit dns-name {contains</td>
<td>exact (mark)</td>
</tr>
<tr>
<td>dns-name</td>
<td>Matches any hostname which has this DNS label. (for example <em>.test.</em>)</td>
</tr>
<tr>
<td>contains</td>
<td>Matches an exact hostname in the network-service</td>
</tr>
<tr>
<td>exact</td>
<td>Matches any hostname as suffix (for example *.test)</td>
</tr>
<tr>
<td>suffix</td>
<td>Identifies a specific host (as the source to match) by its domain name. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are forwarded.</td>
</tr>
<tr>
<td>log</td>
<td>Logs all permit events matching this dns entry. If a dns-name is matched an event is logged.</td>
</tr>
<tr>
<td>mark [8021p &lt;0-7&gt;</td>
<td>dscp &lt;0-63&gt;]</td>
</tr>
<tr>
<td>• 8021p &lt;0-7&gt;</td>
<td>Marks packets by modifying 802.1.p VLAN user priority</td>
</tr>
<tr>
<td>• dscp &lt;0-63&gt;</td>
<td>Marks packets by modifying DSCP TOS bits in the header</td>
</tr>
<tr>
<td>rule-precedence &lt;1-5000&gt;</td>
<td>The following keywords are recursive and common to all of the above parameters:</td>
</tr>
<tr>
<td>• rule-precedence</td>
<td>Assigns a precedence for this deny rule</td>
</tr>
<tr>
<td>• &lt;1-5000&gt;</td>
<td>Specify a value from 1 - 5000.</td>
</tr>
<tr>
<td>Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</td>
<td></td>
</tr>
<tr>
<td>• rule-description</td>
<td>Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</td>
</tr>
<tr>
<td>Permit Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>permit icmp</code></td>
<td>Applies this permit rule to ICMP packets only</td>
</tr>
<tr>
<td><code>&lt;SOURCE-IP/MASK&gt;</code></td>
<td>Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are permitted.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code></td>
<td>Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are permitted.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code></td>
<td>Specify the network-group alias name (should be existing and configured).</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the source as any source IP address. ICMP packets received from any source are permitted.</td>
</tr>
<tr>
<td><code>from-vlan &lt;VLAN-ID&gt;</code></td>
<td>Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are permitted.</td>
</tr>
<tr>
<td><code>&lt;VLAN-ID&gt;</code></td>
<td>Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</td>
</tr>
<tr>
<td><code>host &lt;SOURCE-HOST-IP&gt;</code></td>
<td>Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are permitted.</td>
</tr>
<tr>
<td><code>&lt;SOURCE-HOST-IP&gt;</code></td>
<td>Specify the source host’s exact IP address in the A.B.C.D format.</td>
</tr>
<tr>
<td><code>&lt;DEST-IP/MASK&gt;</code></td>
<td>Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are permitted.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code></td>
<td>Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are permitted.</td>
</tr>
<tr>
<td><code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code></td>
<td>Specify the network-group alias name (should be existing and configured).</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the destination as any destination IP address. ICMP packets addressed to any destination are permitted.</td>
</tr>
<tr>
<td><code>host &lt;DEST-HOST-IP&gt;</code></td>
<td>Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are permitted.</td>
</tr>
<tr>
<td><code>&lt;DEST-HOST-IP&gt;</code></td>
<td>Specify the destination host’s exact IP address in the A.B.C.D format.</td>
</tr>
<tr>
<td><code>&lt;ICMP-TYPE&gt;</code></td>
<td>Defines the ICMP packet type. For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.</td>
</tr>
<tr>
<td><code>&lt;ICMP-CODE&gt;</code></td>
<td>Defines the ICMP message type. For example, an ICMP code 3 indicates “Destination Unreachable”, code 1 indicates “Host Unreachable”, and code 3 indicates “Port Unreachable.”</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</td>
</tr>
</tbody>
</table>
**permit ip** [ \(<\text{SOURCE-IP/\text{MASK}}>|\<\text{NETWORK-GROUP-ALIAS-NAME}|\text{any}|\text{from-vlan }<\text{VLAN-ID}|\text{host }<\text{SOURCE-HOST-IP}>\) ] [ \(<\text{DEST-IP/\text{MASK}}>|\<\text{NETWORK-GROUP-ALIAS-NAME}|\text{any}|\text{host }<\text{DEST-HOST-IP}>\) ] (log, rule-precedence \(<1-5000>\)) \{(\text{rule-description }<\text{LINE}>\)}

**rule-precedence** \(<1-5000>\)
**rule-description** \(<\text{LINE}>\)

The following keywords are recursive and common to all of the above parameters:
- **rule-precedence** – Assigns a precedence for this permit rule
  - \(<1-5000>\) – Specify a value from 1 - 5000.
  
  **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
- **rule-description** – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

**ip**
Applies this permit rule to IP packets only

**\(<\text{SOURCE-IP/\text{MASK}}>|\<\text{NETWORK-GROUP-ALIAS-NAME}|\text{any}|\text{from-vlan }<\text{VLAN-ID}|\text{host }<\text{SOURCE-HOST-IP}>\)**
Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are permitted.

**\(<\text{NETWORK-GROUP-ALIAS-NAME}>\)**
Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are permitted.
- **\(<\text{NETWORK-GROUP-ALIAS-NAME}>\)** – Specify the network-group alias name (should be existing and configured).

**any**
Specifies the source as any source IP address. IP packets received from any source are permitted.

**from-vlan**
\(<\text{VLAN-ID}>\)
Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are permitted.
- **\(<\text{VLAN-ID}>\)** – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).
  
  **Note:** Use this option with WLANs and port ACLs.

**host**
\(<\text{SOURCE-HOST-IP}>\)
Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are permitted.
- **\(<\text{SOURCE-HOST-IP}>\)** – Specify the source host’s exact IP address in the A.B.C.D format.

**\(<\text{DEST-IP/\text{MASK}}>|\<\text{NETWORK-GROUP-ALIAS-NAME}>\)**
Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are permitted.

**any**
Specifies the destination as any destination IP address. IP packets addressed to any destination are permitted.

**host**
\(<\text{DEST-HOST-IP}>\)
Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are permitted.
- **\(<\text{DEST-HOST-IP}>\)** – Specify the destination host’s exact IP address in the A.B.C.D format.

**\(<\text{NETWORK-GROUP-ALIAS-NAME}>\)**
Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are permitted.
- **\(<\text{NETWORK-GROUP-ALIAS-NAME}>\)** – Specify the network-group alias name (should be existing and configured).

**log**
Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule-precedence &lt;1-5000&gt;</td>
<td>The following keywords are recursive and common to all of the above parameters:</td>
</tr>
<tr>
<td>rule-description &lt;LINE&gt;</td>
<td>• rule-precedence – Assigns a precedence for this permit rule</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</td>
</tr>
<tr>
<td></td>
<td>• rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</td>
</tr>
</tbody>
</table>

• permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,rule-precedence <1-5000>)

<table>
<thead>
<tr>
<th>protocol</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proto</td>
<td>Configures the ACL for additional protocols</td>
</tr>
<tr>
<td></td>
<td>Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter</td>
</tr>
<tr>
<td>&lt;PROTOCOL-NUMBER&gt;</td>
<td>Filters protocols using their IANA protocol number</td>
</tr>
<tr>
<td></td>
<td>• &lt;PROTOCOL-NUMBER&gt; – Specify the protocol number.</td>
</tr>
<tr>
<td>&lt;PROTOCOL-NAME&gt;</td>
<td>Filters protocols using their IANA protocol name</td>
</tr>
<tr>
<td></td>
<td>• &lt;PROTOCOL-NAME&gt; – Specify the protocol name.</td>
</tr>
<tr>
<td>eigrp</td>
<td>Identifies the EIGRP protocol (number 88)</td>
</tr>
<tr>
<td></td>
<td>EIGRP enables routers to maintain copies of neighbors’ routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.</td>
</tr>
<tr>
<td>gre</td>
<td>Identifies the GRE protocol (number 47)</td>
</tr>
<tr>
<td></td>
<td>GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.</td>
</tr>
<tr>
<td>igmp</td>
<td>Identifies the IGMP protocol (number 2)</td>
</tr>
<tr>
<td></td>
<td>IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.</td>
</tr>
<tr>
<td>igp</td>
<td>Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9)</td>
</tr>
<tr>
<td></td>
<td>IGP enables exchange of information between hosts and routers within a managed network. The most commonly used interior gateway protocol (IGP) protocols are: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>ospf</td>
<td>Identifies the OSPF protocol (number 89)</td>
</tr>
<tr>
<td></td>
<td>OSPF is a link-state interior gateway protocol (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.</td>
</tr>
</tbody>
</table>
| **vrrp** | Identifies the VRRP protocol (number 112)
VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;SOURCE-IP/MASK&gt;</strong></td>
<td>Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are permitted.</td>
</tr>
</tbody>
</table>
| **<NETWORK-GROUP-ALIAS-NAME>** | Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are permitted.
- **<NETWORK-GROUP-ALIAS-NAME>** – Specify the network-group alias name (should be existing and configured). |
| **any** | Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are permitted. |
| **from-vlan** | Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are permitted.
- **<VLAN-ID>** – Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20).
**Note:** Use this option with WLANs and port ACLs. |
| **host** | Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are permitted.
- **<SOURCE-HOST-IP>** – Specify the source host’s exact IP address in the A.B.C.D format. |
| **<DEST-IP/MASK>** | Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are permitted. |
| **any** | Specifies the destination as any destination IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are permitted. |
| **host** | Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are permitted.
- **<SOURCE-HOST-IP>** – Specify the destination host’s exact IP address in the A.B.C.D format. |
| **<NETWORK-GROUP-ALIAS-NAME>** | Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are permitted.
- **<NETWORK-ALIAS-NAME>** – Specify the network-group alias name (should be existing and configured).
**Note:** After specifying the source and destination IP address(es), specify the action taken in case of a match. |
| **log** | Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged. |
The following keywords are recursive and common to all of the above parameters:

- **rule-precedence** – Assigns a precedence for this permit rule
- **<1-5000>** – Specify a value from 1 - 5000.

**Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.

- **rule-description** – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Applies this permit rule to TCP packets only</td>
</tr>
<tr>
<td>udp</td>
<td>Applies this deny rule to UDP packets only</td>
</tr>
<tr>
<td>&lt;SOURCE-IP/MASK&gt;</td>
<td>This keyword is common to the 'tcp' and 'udp' parameters.</td>
</tr>
<tr>
<td></td>
<td>Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP</td>
</tr>
<tr>
<td></td>
<td>packets received from the specified sources are permitted.</td>
</tr>
<tr>
<td>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are permitted.</td>
</tr>
<tr>
<td></td>
<td>• &lt;NETWORK-ALIAS-GROUP-NAME&gt; – Specify the network-group alias name</td>
</tr>
<tr>
<td></td>
<td>(should be existing and configured).</td>
</tr>
<tr>
<td></td>
<td>After specifying the source and destination IP address(es), specify the</td>
</tr>
<tr>
<td></td>
<td>action taken in case of a match.</td>
</tr>
<tr>
<td>any</td>
<td>This keyword is common to the 'tcp' and 'udp' parameters.</td>
</tr>
<tr>
<td></td>
<td>Specifies the source as any source IP address. TCP/UDP packets received</td>
</tr>
<tr>
<td></td>
<td>from any source are permitted.</td>
</tr>
<tr>
<td>from-vlan &lt;VLAN-ID&gt;</td>
<td>This keyword is common to the 'tcp' and 'udp' parameters.</td>
</tr>
<tr>
<td></td>
<td>Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP</td>
</tr>
<tr>
<td></td>
<td>packets received from the VLANs identified here are permitted.</td>
</tr>
<tr>
<td></td>
<td>• &lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the</td>
</tr>
<tr>
<td></td>
<td>start and end VLAN IDs separated by a hyphen (for example, 12-20).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use this option with WLANs and port ACLs.</td>
</tr>
<tr>
<td>host &lt;SOURCE-HOST-IP&gt;</td>
<td>Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are permitted.</td>
</tr>
<tr>
<td></td>
<td>• &lt;SOURCE-HOST-IP&gt; – Specify the source host’s exact IP address in the</td>
</tr>
<tr>
<td></td>
<td>A.B.C.D format.</td>
</tr>
<tr>
<td>&lt;DEST-IP/MASK&gt;</td>
<td>This keyword is common to the 'tcp' and 'udp' parameters.</td>
</tr>
<tr>
<td></td>
<td>Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP</td>
</tr>
<tr>
<td></td>
<td>packets addressed to the specified destinations are permitted.</td>
</tr>
<tr>
<td>any</td>
<td>This keyword is common to the 'tcp' and 'udp' parameters.</td>
</tr>
<tr>
<td></td>
<td>Specifies the destination as any destination IP address. TCP/UDP packets</td>
</tr>
<tr>
<td></td>
<td>received from any destination are permitted.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>eq &lt;SOURCE-PORT&gt;</td>
<td>Identifies a specific source port&lt;br&gt;• &lt;SOURCE-PORT&gt; – Specify the exact source port.</td>
</tr>
<tr>
<td>host &lt;DEST-HOST-IP&gt;</td>
<td>Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are permitted.&lt;br&gt;• &lt;DEST-HOST-IP&gt; – Specify the destination host’s exact IP address in the A.B.C.D format.</td>
</tr>
<tr>
<td>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>This keyword is common to the ‘tcp’ and ‘udp’ parameters.&lt;br&gt;Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are permitted.&lt;br&gt;• &lt;NETWORK-ALIAS-GROUP-NAME&gt; – Specify the network-group alias name (should be existing and configured).</td>
</tr>
<tr>
<td>range &lt;START-PORT&gt; &lt;END-PORT&gt;</td>
<td>Specifies a range of source ports&lt;br&gt;• &lt;START-PORT&gt; – Specify the first port in the range.&lt;br&gt;• &lt;END-PORT&gt; – Specify the last port in the range.</td>
</tr>
<tr>
<td>eq [1-65535]</td>
<td>Identifies a specific destination or protocol port to match&lt;br&gt;• 1-65535 – The destination port is designated by its number&lt;br&gt;• &lt;SERVICE-NAME&gt; – Specifies the service name&lt;br&gt;• bgp – The designated Border Gateway Protocol (BGP) protocol port (179)&lt;br&gt;• dns – The designated Domain Name System (DNS) protocol port (53)&lt;br&gt;• ftp – The designated File Transfer Protocol (FTP) protocol port (21)&lt;br&gt;• ftp-data – The designated FTP data port (20)&lt;br&gt;• gropher – The designated GROPERHER protocol port (70)&lt;br&gt;• https – The designated HTTPS protocol port (443)&lt;br&gt;• ldap – The designated Lightweight Directory Access Protocol (LDAP) protocol port (389)&lt;br&gt;• nntp – The designated Network News Transfer Protocol (NNTP) protocol port (119)&lt;br&gt;• ntp – The designated Network Time Protocol (NTP) protocol port (123)&lt;br&gt;• pop3 – The designated POP3 protocol port (110)&lt;br&gt;• sip – The designated Session Initiation Protocol (SIP) protocol port (5060)&lt;br&gt;• smtp – The designated Simple Mail Transfer Protocol (SMTP) protocol port (25)&lt;br&gt;• ssh – The designated Secure Shell (SSH) protocol port (22)&lt;br&gt;• telnet – The designated Telnet protocol port (23)&lt;br&gt;• tftp – The designated Trivial File Transfer Protocol (TFTP) protocol port (69)&lt;br&gt;• www – The designated www protocol port (80)</td>
</tr>
<tr>
<td>range &lt;START-PORT&gt; &lt;END-PORT&gt;</td>
<td>Specifies a range of destination ports&lt;br&gt;• &lt;START-PORT&gt; – Specify the first port in the range.&lt;br&gt;• &lt;END-PORT&gt; – Specify the last port in the range.</td>
</tr>
<tr>
<td>log</td>
<td>Logs all permit events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list. The following protocols are supported:

- IP
- ICMP
- ICP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. The packet is allowed or denied based on the ACL configuration.

- Filtering on TCP or UDP allows you to specify port numbers as filtering criteria.
- Select ICMP to allow/deny packets. Selecting ICMP filters ICMP packets based on ICMP type and code.

**Note:** The log option is functional only for router ACL’s. The log option displays an informational logging message about the packet matching the entry sent to the console.

### Examples

```
 rfs7000-37FABE(config-ip-acl-test)#show context
 ip access-list test
 rfs7000-37FABE(config-ip-acl-test)#

 rfs7000-37FABE(config-ip-acl-test)#permit ip 172.16.10.0/24 any log rule-precedence 750
 rfs7000-37FABE(config-ip-acl-test)#permit tcp 172.16.10.0/24 any log rule-precedence 800

 rfs7000-37FABE(config-ip-acl-test)#show context
 ip access-list test
   permit ip 172.16.10.0/24 any log rule-precedence 750
   permit tcp 172.16.10.0/24 any log rule-precedence 800
 rfs7000-37FABE(config-ip-acl-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes a specified IP permit access rule</td>
</tr>
<tr>
<td>alias</td>
<td>Creates and configures aliases (network, VLAN, and service)</td>
</tr>
</tbody>
</table>
11.2 mac-access-list

ACCESS-LIST

The following table summarizes MAC Access list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a new deny access rule or modifies an existing rule. A deny access rule marks packets for rejection.</td>
<td>page 11-33</td>
</tr>
<tr>
<td>disable</td>
<td>Disables a MAC deny or permit rule without removing it from the ACL</td>
<td>page 11-36</td>
</tr>
<tr>
<td>ex3500</td>
<td>Creates a MAC ACL deny and/or permit rule applicable only to the EX3500 switch</td>
<td>page 11-38</td>
</tr>
<tr>
<td>insert</td>
<td>Inserts a rule in an MAC ACL without overwriting or replacing an exciting rule having the same precedence</td>
<td>page 11-41</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny and/or a permit access rule from a MAC ACL</td>
<td>page 11-43</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a new permit access rule or modifies an existing rule. A deny access rule marks packets for forwarding.</td>
<td>page 11-44</td>
</tr>
</tbody>
</table>
11.2.1 deny

**mac-access-list**

Creates a deny rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for rejection. You can also use this command to modify an existing deny rule.

---

**NOTE:** Use a decimal value representation to implement a *permit/deny* designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

---

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>][<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>](dot1p <0-7>,type [8021q|<1-65535]|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence <1-5000>) {rule-description <LINE>}
```

**Parameters**
- `deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>][<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>](dot1p <0-7>,type [8021q|<1-65535]|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence <1-5000>) {rule-description <LINE>}`

<SOURCE-MAC> <SOURCE-MAC-MASK>
- Configures the source MAC address and mask to match
  - `<SOURCE-MAC>` – Specify the source MAC address to match.
  - `<SOURCE-MAC-MASK>` – Specify the source MAC address mask.
  - Packets received from the specified MAC addresses are dropped.

any
- Identifies all devices as the source to deny access. Packets received from any source are dropped.

host <SOURCE-HOST-MAC>
- Identifies a specific host as the source to deny access
  - `<SOURCE-HOST-MAC>` – Specify the source host’s exact MAC address to match.
  - Packets received from the specified host are dropped.

<DEST-MAC> <DEST-MAC-MASK>
- Configures the destination MAC address and mask to match
  - `<DEST-MAC>` – Specify the destination MAC address to match.
  - `<DEST-MAC-MASK>` – Specify the destination MAC address mask to match.
  - Packets addressed to the specified MAC addresses are dropped.

any
- Identifies all devices as the destination to deny access. Packets addressed to any destination are dropped.

host <DEST-HOST-MAC>
- Identifies a specific host as the destination to deny access
  - `<DEST-HOST-MAC>` – Specify the destination host’s exact MAC address to match.
  - Packets addressed to the specified host are dropped.

dotp1p <0-7>
- Configures the 802.1p priority value. Sets the service classes for traffic handling
  - `<0-7>` – Specify 802.1p priority from 0 - 7.
Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and EtherType.

- ARP
- WISP
- IP
- 802.1q

**NOTE:** MAC ACLs always take precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed or denied based on the ACL's configuration.
Examples

```
rfs4000-229D58(config-mac-acl-test)#deny 41-85-45-89-66-77 ff-ff-ff-00-00-00 any vlan 1 rule-precedence 1
rfs4000-229D58(config-mac-acl-test)#deny host 00-01-ae-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#show context mac access-list test
deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
deny host 00-01-AE-00-22-11 any rule-precedence 2
```

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
rfs7000-37FABE(config-mac-acl-test)#deny any host 00:01:ae:00:22:11
```

The following example denies traffic between two hosts based on MAC addresses:

```
rfs7000-37FABE(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host 01:02:89:78:78:45
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a specified MAC deny access rule</td>
</tr>
</tbody>
</table>
11.2.2 disable

Disables a MAC deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

disable [deny|insert|permit]

disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] {dot1p <0-7>, mark [8021p <0-7>|dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>} log (rule-precedence <1-5000>) {(rule-description <LINE>)}

disable insert [deny|permit]

Parameters

- disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] {dot1p <0-7>, mark [8021p <0-7>|dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>} log (rule-precedence <1-5000>) {(rule-description <LINE>)}

| disable [deny|insert|permit] | Disables a deny, insert or permit access rule without removing it from the MAC ACL |
|-----------------------------|----------------------------------------------------------------------------------|
| <SOURCE-MAC> <SOURCE-MAC-MASK> | Specifies the source MAC address and mask to match |
| • <SOURCE-MAC> – Specify the source MAC address to match. |
| • <SOURCE-MAC-MASK> – Specify the source MAC address mask. |
| any | Select ‘any’ if the rule is applicable to any source MAC address |
| host <SOURCE-HOST-MAC> | Specify the source host’s exact MAC address |
| <DEST-MAC> <DEST-MAC-MASK> | Specifies the destination MAC address and mask to match |
| • <DEST-MAC> – Specify the destination MAC address. |
| • <DEST-MAC-MASK> – Specify the destination MAC address mask. |
| any | Select ‘any’ if the rule is applicable to any destination MAC address |
| host <DEST-HOST-MAC> | Specify the destination host’s exact MAC address |
| log | The following keyword defines the action taken when a packet matches any or all of the above specified criteria |
| • log – Logs a record. when a packet matches the specified criteria |
| dot1p <0-7> | Specify the 802.1p priority from 0 - 7 |
### Examples

The following example shows the MAC access list 'test' settings before the 'disable' command is executed:

```bash
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

The following example shows the MAC access list 'test' settings after the 'disable' command is executed:

```bash
rfs4000-229D58(config-mac-acl-test)#disable deny host 00-01-AE-00-22-11 any rule-precedence 2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Enables a disabled deny or permit rule</td>
</tr>
<tr>
<td><strong>deny</strong></td>
<td>Creates a new deny access rule or modifies an existing rule</td>
</tr>
<tr>
<td><strong>permit</strong></td>
<td>Creates a new permit access rule or modifies an existing rule</td>
</tr>
</tbody>
</table>
11.2.3 ex3500

*mac-access-list*

Creates a MAC ACL deny and/or permit rule, applicable only to the EX3500 switch.

Each deny or permit rule consists of a set of match criteria and an associated action, which is deny access for the deny rule and allow access for the permit rule. When applied to layer 2 traffic (between a EX3500 switch and the WiNG managed service platform or a WiNG VM interface) every packet is matched against the configured match criteria and in case of a match the packet is dropped or forwarded depending on the rule type.

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and command line interface (CLI), which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

**NOTE:** To implement the EX3500 MAC ACL rule, apply the MAC ACL directly to a EX3500 device, or to an EX35XX profile. For more information see, *access-group*.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2]

    ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2] [any | host <SOURCE-MAC>| network <SOURCE-MAC> <SOURCE-MAC-MASK>] [any | host <DEST-MAC>| network <DEST-MAC> <DEST-MAC-MASK>] [ethertype <0-65535|ethertype-mask <0-65535> | ex3500-time-range <TIME-RANGE-NAME>|rule-precedence <1-128>|vlan <1-4094>| vlan-mask <1-4095>]

**Parameters**

- ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2] [any | host <SOURCE-MAC>| network <SOURCE-MAC> <SOURCE-MAC-MASK>] [any | host <DEST-MAC>| network <DEST-MAC> <DEST-MAC-MASK>] [ethertype <0-65535|ethertype-mask <0-65535> | ex3500-time-range <TIME-RANGE-NAME>|rule-precedence <1-128>|vlan <1-4094>| vlan-mask <1-4095>]

| [deny|permit] | Creates a deny or permit MAC ACL rule and configures the rule parameters. Every EX3500 MAC ACL rule provides a set of match criteria against which incoming and outgoing packets (to and from an EX3500 device) are matched. In case of a match, the packet is dropped or forwarded depending on the rule type. The packet is dropped in case of a *deny* rule, and forwarded for an *permit* rule. |
| [all|tagged-eth2|untagged-eth2] | Specifies the packet type |
| all | Applies this deny/permit rule to all packets |
| tagged-eth2 | Applies this deny/permit rule only to tagged Ethernet-2 packets |
| untagged-eth2 | Applies this deny/permit rule only to untagged Ethernet-2 packets |

After specifying the packet type, configure the source and/or EX3500 MAC addresses to match.
Enter the **Source** MAC addresses
- `any` – Identifies all EX3500 devices as a source to match
- `host <SOURCE-MAC>` – Identifies a specific EX3500 host as the source to match
- `<SOURCE-MAC>` – Specify the source host’s exact MAC address
- `network <SOURCE-MAC> <SOURCE-MAC-MASK>` – Configures a range of MAC addresses as the source to match. Packets received from any of these MAC addresses are dropped.
  - `<SOURCE-MAC>` – Specify the source MAC address to match.
  - `<SOURCE-MAC-MASK>` – Specify the source MAC bit mask.

For a deny rule, packets received from EX3500 device(s) matching the specified MAC address(es) are dropped.

For a permit rule, packets received from EX3500 device(s) matching the specified MAC address(es) are forwarded.

Enter the **Destination** MAC addresses
- `any` – Identifies all EX3500 devices as a destination to match
- `host <SOURCE-MAC>` – Identifies a specific EX3500 host as the destination to match
- `<SOURCE-MAC>` – Specify the destination host’s exact MAC address
- `network <SOURCE-MAC> <SOURCE-MAC-MASK>` – Configures a range of MAC addresses as the destination to match. Packets addressed to any of these MAC addresses are dropped.
  - `<SOURCE-MAC>` – Specify the destination MAC address to match.
  - `<SOURCE-MAC-MASK>` – Specify the destination MAC bit mask.

For a deny rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are dropped.

For a permit rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are forwarded.

**ether-type**
- `<0-65535>` – Specify the value from 0 - 65535. The default value is 1.

**ethertype-mask**
- `<0-65535>` – Specify the value from 0 - 65535. The default value is 1.

**ex3500-time-range**
- `<TIME-RANGE-NAME>` – Specify the time range name.

An EX3500 time range list consists of a set of periodic and absolute time range rules. Periodic time ranges recur periodically at specified time periods, such as daily, weekly, weekends, weekdays, and on specific week days, for example on every successive Mondays. Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period (the starting and ending days and time are fixed).

**Note:** For information on configuring EX3500 time-range, see **ex3500**.

**vlan**
- `<1-4094>` – Specify the VLAN ID from 1 - 4094.

**vlan-mask**
- `<1-4095>` – Specify the VLAN bit mask from 1 - 4095.
### rule-precedence

<table>
<thead>
<tr>
<th>&lt;1-128&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures a precedence for this EX3500 MAC ACL</td>
</tr>
<tr>
<td>• &lt;1 - 128&gt; – Specify a value from 1 - 128. ACLs with lower precedence are applied first to packets.</td>
</tr>
</tbody>
</table>

#### Examples

```
nx9500-6C8809(config-mac-acl-ex3500MacACL)#ex3500 deny tagged-eth2 any any vlan 20 rule-precedence 1

nx9500-6C8809(config-mac-acl-ex3500MacACL)#show context
mac access-list ex3500MacACL
  ex3500 deny tagged-eth2 any any vlan 20 rule-precedence 1
nx9500-6C8809(config-mac-acl-ex3500MacACL)#
```
11.2.4 insert

mac-access-list

Enables the insertion of a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence. The insert option allows a new rule to be inserted within a MAC ACL. Consider an MAC ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule’s precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.

NOTE: NOT using insert when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
insert [deny|permit] <PARAMETERS> (dot1p <0-7>,mark [8021p <0-7>|dscp <0-63>],
    type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,
    log,rule-precedence <1-5000>) {rule-description <LINE>}
```

Parameters

- `insert [deny|permit] <PARAMETERS>`<PARAMETERS> (dot1p <0-7>,mark [8021p <0-7]|dscp <0-63>],
  type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,
  log,rule-precedence <1-5000>) {rule-description <LINE>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;PARAMETERS&gt;</code></td>
<td>Provides the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see <code>deny</code>. For more information on the permit rule, see <code>permit</code>.</td>
</tr>
<tr>
<td><code>dot1p &lt;0-7&gt;</code></td>
<td>Configures the 802.1p priority value. Sets the service classes for traffic handling</td>
</tr>
<tr>
<td>`mark [8021p &lt;0-7]</td>
<td>dscp &lt;0-63&gt;`</td>
</tr>
</tbody>
</table>

- 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7
- dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63

**Note:** This option is applicable only to the `insert > permit` MAC ACL rule.
### Examples

```bash
rfs4000-229D58(config-mac-acl-test1)#deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
rfs4000-229D58(config-mac-acl-test1)#deny host B4-C7-99-6D-CD-9B any rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
deny host B4-C7-99-6D-CD-9B any rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#

In the following example a new rule is inserted between the rules having precedences 1 and 2. The precedence of the existing precedence ‘2’ rule changes to precedence 3.

```bash
rfs4000-229D58(config-mac-acl-test1)#insert permit host B4-C7-99-6D-B5-D6 host B4-C7-99-6D-CD-9B rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
permit host B4-C7-99-6D-B5-D6 host B4-C7-99-6D-CD-9B rule-precedence 2
deny host B4-C7-99-6D-CD-9B any rule-precedence 3
rfs4000-229D58(config-mac-acl-test1)#
```
11.2.5 no

mac-access-list

Negates a command or sets its default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|disable|permit]

no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]

[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>]

(dot1p <0-7>, mark [8021p <0-7]|dscp <0-63>], type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp], vlan <1-4095>) log (rule-precedence <1-5000>)

{(rule-description <LINE>)}

no disable [deny|permit] <RULE-PARAMETERS>

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes a deny or permit rule from the MAC ACL |

Examples

rfs7000-37FABE(config-mac-acl-test)#show context
mac access-list test
    permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
    permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610
deny any host 33-44-55-66-77-88 log rule-precedence 700

rfs7000-37FABE(config-mac-acl-test)#no deny any host 33-44-55-66-77-88 log rule-precedence 700

rfs7000-37FABE(config-mac-acl-test)#show context
mac access-list test
    permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
    permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610
### 11.2.6 permit

*mac-access-list*

Creates a permit rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for forwarding. You can also use this command to modify an existing permit rule.

#### NOTE:

Use a decimal value representation to implement a permit/deny designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
  [<DEST-MAC<DEST-MAC-MASK>|any|host <DEST-HOST-MAC>]
  (dot1p <0-7>,mark [8021p <0-7>,dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log (rule-precedence <1-5000>){(rule-description <LINE>)}
```

#### Parameters

- **permit**
  - `<SOURCE-MAC>`
  - `<SOURCE-MAC-MASK>`
  - any
  - host `<SOURCE-HOST-MAC>`
  - `<DEST-MAC>`
  - `<DEST-MAC-MASK>`
  - (dot1p `<0-7>`, mark [8021p `<0-7>`, dscp `<0-63>`], type [8021q|`<1-65535>`|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp], vlan `<1-4095>`)
  - log (rule-precedence `<1-5000>`)
  - (rule-description `<LINE>`)

<table>
<thead>
<tr>
<th><code>&lt;SOURCE-MAC&gt;</code></th>
<th><code>&lt;SOURCE-MAC-MASK&gt;</code></th>
<th><code>&lt;DEST-MAC&gt;</code></th>
<th><code>&lt;DEST-MAC-MASK&gt;</code></th>
<th><code>any</code></th>
<th><code>host</code> <code>&lt;SOURCE-HOST-MAC&gt;</code></th>
<th><code>host</code> <code>&lt;DEST-HOST-MAC&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the source MAC address and mask to match</td>
<td>• <code>&lt;SOURCE-MAC&gt;</code> – Specify the source MAC address to match.</td>
<td>• <code>&lt;SOURCE-MAC-MASK&gt;</code> – Specify the source MAC address mask.</td>
<td>Packets addressed to the specified MAC addresses are forwarded.</td>
<td>Identifies all devices as the source to permit access. Packets addressed from any source are forwarded.</td>
<td>Identifies a specific host as the source to permit access</td>
<td>Identifies the source host’s exact MAC address to match. Packets addressed to the specified host are forwarded.</td>
</tr>
<tr>
<td><code>&lt;DEST-MAC&gt;</code></td>
<td><code>&lt;DEST-MAC-MASK&gt;</code></td>
<td><code>any</code></td>
<td><code>host</code> <code>&lt;DEST-HOST-MAC&gt;</code></td>
<td>Configures the destination MAC address and mask to match</td>
<td>• <code>&lt;DEST-MAC&gt;</code> – Specify the destination MAC address to match.</td>
<td>• <code>&lt;DEST-MAC-MASK&gt;</code> – Specify the destination MAC address mask to match. Packets addressed to the specified MAC addresses are forwarded.</td>
</tr>
<tr>
<td>Specifies the destination MAC address mask to match</td>
<td><code>any</code></td>
<td><code>host</code> <code>&lt;DEST-HOST-MAC&gt;</code></td>
<td>Identifies a specific host as the destination to permit access</td>
<td>Identifies the destination host’s exact MAC address to match. Packets addressed to the specified host are forwarded.</td>
<td>Identifies a specific host as the destination to permit access</td>
<td>Identifies the destination host’s exact MAC address to match. Packets addressed to the specified host are forwarded.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| dotp1p <0-7>       | Configures the 802.1p priority value. Sets the service classes for traffic handling  
• <0-7> – Specify 802.1p priority from 0 - 7.                                                                                          |
| mark [8021p <0-7>, dscp <0-63>] | Marks/modifies packets that match the criteria specified here  
• 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7  
• dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63  
**Note:** This option is applicable only to the MAC ACL permit rule. |
| type [8021q|<1-65535>| aarp|appletalk| arpl|ipv6|ipv|mint| rarp|wisp] | Configures the EtherType value  
An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are:  
• 8021q – Indicates a 802.1q payload (0x8100)  
• <1-65535> – Indicates the EtherType protocol number  
• aarp – Indicates the Appletalk *Address Resolution Protocol* (ARP) payload (0x80F3)  
• appletalk – Indicates the Appletalk Protocol payload (0x809B)  
• arp – Indicates the ARP payload (0x0806)  
• ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800)  
• ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD)  
• ipx – Indicates the Novell’s IPX payload (0x8137)  
• mint – Indicates the MiNT protocol payload (0x8783)  
• rarp – Indicates the reverse *Address Resolution Protocol* (ARP) payload (0x8035)  
• wisp – Indicates the *Wireless Internet Service Provider* (WISP) payload (0x8783) |
| vlan <1-4095>     | Configures the VLAN ID  
• <1-4095> – Specify the VLAN ID from 1 - 4095.                                                                                                                                                 |
| log                | Logs all permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is addressed to a specified MAC address or is destined for a specified MAC address), an event is logged. |
| rule-precedence <1-5000> | The following keywords are recursive and common to all of the above parameters:  
• rule-precedence – Assigns a precedence for this permit rule  
• <1-5000> – Specify a value from 1 - 5000.  
**Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.  
• rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |
Usage Guidelines
The permit command in the MAC ACL allows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, or Ethernet type. Common types include:

- ARP
- WISP
- IP
- 802.1q

Layer 2 traffic is not allowed by default. To adopt an access point through an interface, configure an ACL to allow an Ethernet WISP.

Use the mark option to specify the type of service (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL’s configuration.

NOTE: To apply an IP based ACL to an interface, a MAC access list entry is mandatory to allow ARP. A MAC ACL always takes precedence over IP based ACLs.

Examples

rfs7000-37FABE(config-mac-acl-test)#permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600

rfs7000-37FABE(config-mac-acl-test)#permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610

rfs7000-37FABE(config-mac-acl-test)#show context
mac access-list testPF
  permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
  permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610

rfs7000-37FABE(config-mac-acl-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes or resets a specified MAC ACL permit rule</td>
</tr>
</tbody>
</table>
11.3 ipv6-access-list

ACCESS-LIST

Configures a IPv6 ACL

An IPv6 ACL defines a set of rules that filter IPv6 packets flowing through a port or interface. Each rule specifies the action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

The WiNG software supports IPv6 only on VLAN interfaces. Therefore, IPv6 ACLs can be applied only on the VLAN interface.

The following table summarizes IPv6 access list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a deny access rule or modifies an existing rule. A deny access rule rejects IPv6 packets from specified address(es) and/or destined for specified address(es).</td>
<td>page 11-48</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny and/or a access rule from a IPv6 ACL</td>
<td>page 11-53</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a permit access rule or modifies an existing rule. A permit access rule accepts IPv6 packets from specified address(es) and/or destined for specified address(es).</td>
<td>page 11-54</td>
</tr>
</tbody>
</table>
11.3.1 deny

`ipv6-access-list`

Creates a deny rule that rejects packets from a specified IPv6 source and/or to a specified IPv6 destination. You can also use this command to modify an existing deny rule.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

deny [icmpv6|ipv6|proto|tcp|udp]


**Parameters**


<table>
<thead>
<tr>
<th>icmpv6</th>
<th>Applies this deny rule to ICMPv6 packets only</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;SOURCE-IPv6/MASK&gt;</code></td>
<td>Specifies a range of IPv6 source address (network) to match. ICMPv6 packets received from any source in the specified network are dropped.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the source as any IPv6 address. ICMPv6 packets received from any source are dropped.</td>
</tr>
<tr>
<td>host <code>&lt;SOURCE-HOST-IPv6&gt;</code></td>
<td>Identifies a specific host (as the source to match) by its IPv6 address. ICMPv6 packets received from the specified host are dropped.</td>
</tr>
<tr>
<td><code>&lt;DEST-IPv6/MASK&gt;</code></td>
<td>Specifies a range of IPv6 destination address (network) to match. ICMPv6 packets addressed to any destination within the specified network are dropped.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the destination as any IPv6 address. ICMPv6 packets addressed to any destination are dropped.</td>
</tr>
<tr>
<td>host <code>&lt;DEST-HOST-IPv6&gt;</code></td>
<td>Identifies a specific host (as the destination to match) by its IPv6 address. ICMPv6 packets addressed to the specified host are dropped.</td>
</tr>
</tbody>
</table>

习惯了这个 deny 命令，你可以使用它来修改现有的 deny 规则。
### <ICMPv6-TYPE> denotes the ICMPv6 type field filter
- **eq** – Configures a specific ICMPv6 type. Specify the ICMPv6 type value.
- **range** – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values.

**Note:** ICMPv6 packets with type field value matching the values specified here are dropped.

### <ICMPv6-CODE> defines the ICMPv6 code field filter
- **eq** – Configures a specific ICMPv6 code. Specify the ICMPv6 code value.
- **range** – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values.

**Note:** ICMPv6 packets with code field value matching the values specified here are dropped.

### log
Logs all deny events matching this entry

### rule-precedence <1-5000>
Assigns a precedence for this deny rule
- **<1-5000>** – Specify a value from 1 - 5000.

**Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.

### rule-description <LINE>
Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

### deny ipv6 [any|host <SOURCE-HOST-IPv6>] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {rule-description <LINE>}

<table>
<thead>
<tr>
<th>ipv6</th>
<th>Applies this deny rule to IPv6 packets only</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SOURCE-IPv6/MASK&gt;</td>
<td>Specifies a range of IPv6 source address (network) to match. IPv6 packets received from any source in the specified network are dropped.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the source as any IPv6 address. IPv6 packets received from any source are dropped.</td>
</tr>
<tr>
<td>host &lt;SOURCE-HOST-IPv6&gt;</td>
<td>Identifies a specific host (as the source to match) by its IPv6 address. IPv6 packets received from the specified host are dropped.</td>
</tr>
<tr>
<td>&lt;DEST-IPv6/MASK&gt;</td>
<td>Specifies a range of IPv6 destination address (network) to match. IPv6 packets addressed to any destination within the specified network are dropped.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the destination as any IPv6 address. IPv6 packets addressed to any destination are dropped.</td>
</tr>
<tr>
<td>host &lt;DEST-HOST-IPv6&gt;</td>
<td>Identifies a specific host (as the destination to match) by its IPv6 address. IPv6 packets addressed to the specified host are dropped.</td>
</tr>
<tr>
<td>log</td>
<td>Logs all deny events matching this entry</td>
</tr>
<tr>
<td>rule-precedence &lt;1-5000&gt;</td>
<td>Assigns a precedence for this deny rule</td>
</tr>
<tr>
<td><strong>&lt;1-5000&gt;</strong></td>
<td>Specify a value from 1 - 5000</td>
</tr>
</tbody>
</table>

**Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
<table>
<thead>
<tr>
<th>rule-description</th>
<th>Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>(proto)</th>
<th>Configures the ACL for additional protocols. Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.</th>
</tr>
</thead>
</table>

- `<PROTOCOL-NUMBER>` | Filters protocols using their Internet Assigned Numbers Authority (IANA) protocol number |
  - `<PROTOCOL-NUMBER>` – Specify the protocol number. |

- `<PROTOCOL-NAME>` | Filters protocols using their IANA protocol name |
  - `<PROTOCOL-NAME>` – Specify the protocol name. |

- `eigrp` | Identifies the EIGRP protocol (number 88) |
  - EIGRP enables routers to maintain copies of neighbors’ routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables. |

- `gre` | Identifies the GRE protocol (number 47) |
  - GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination. |

- `igp` | Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) |
  - IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF. |

- `ospf` | Identifies the OSPF protocol (number 89) |
  - OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. |

- `vrrp` | Identifies the VRRP protocol (number 112) |
  - VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |

- `<SOURCE-IPv6/MASK>` | Specifies a range of IPv6 source address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source in the specified network are dropped. |

- `any` | Specifies the source as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped. |
<table>
<thead>
<tr>
<th>Clause</th>
<th>Description</th>
</tr>
</thead>
</table>
| host <SOURCE-HOST-IPv6> | Identifies a specific host (as the source to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped.  
  • <SOURCE-HOST-IP> – Specify the source host’s exact IPv6 address. |
| <DEST-IPv6/MASK> | Specifies a range of IPv6 destination address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination within the specified network are dropped. |
| any | Specifies the destination as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped. |
| host <DEST-HOST-IPv6> | Identifies a specific host (as the destination to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified host are dropped.  
  • <DEST-HOST-IPv6> – Specify the destination host’s exact IPv6 address. |
| log | Logs all deny events matching this entry |
| rule-precedence <1-5000> | Assigns a precedence for this deny rule  
  • <1-5000> – Specify a value from 1 - 5000.  
  **Note**: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. |
| rule-description <LINE> | Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |

Example deny clauses:

```plaintext
```

tcp | Applies this deny rule to TCP packets only  
udp | Applies this deny rule to UDP packets only  

Example tcp clauses:

```plaintext
```

Example udp clauses:

```plaintext
```

Example eq clauses:

```plaintext
```
### Examples

```
rfs7000-6DCD4B(config-ipv6-acl-test)#deny icmpv6 any any type eq 1 code eq 0 log rule-precedence 1
rfs7000-6DCD4B(config-ipv6-acl-test)#show context ipv6 access-list test
deny_icmpv6 any any type eq destination-unreachable code eq router-renumbering-command log rule-precedence 1
rfs7000-6DCD4B(config-ipv6-acl-test)#
```

### Related Commands

- **no**

  Removes a specified deny access rule
11.3.2 no

- ipv6-access-list

Removes a deny or permit rule

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|permit]

no [deny|permit] [icmpv6|ipv6|proto|tcp|udp] <RULE-PARAMETERS>

{(rule-description <LINE>)}

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes a deny or permit rule from the selected IPv6 access list |

Examples

The following example shows the ACL ‘test’ settings before the ‘no’ commands are executed:

rfs7000-6DCD4B(config-ipv6-acl-test)#show context
ipv6 access-list test
deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-command
log rule-precedence 1
permit proto gre any any log rule-precedence 2
rfs7000-6DCD4B(config-ipv6-acl-test)#

rfs7000-6DCD4B(config-ipv6-acl-test)#no deny icmpv6 any any type eq 1 log rule-precedence 1

rfs7000-6DCD4B(config-ipv6-acl-test)#show context
ipv6 access-list test
permit proto gre any any log rule-precedence 2
rfs7000-6DCD4B(config-ipv6-acl-test)#
11.3.3 permit

Creates a permit rule that accepts packets from a specified IPv6 source and/or to a specified IPv6 destination. You can also use this command to modify an existing permit rule.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

\[
\text{permit [icmpv6|ipv6|proto|tcp|udp]}
\]

\[
\text{permit [icmpv6 | [any|host \langle SOURCE-IPv6/MASK \rangle | host \langle SOURCE-HOST-IPv6 \rangle | \langle DEST-IPv6/MASK \rangle | any|host \langle DEST-HOST-IPv6 \rangle)}
\]

\[
\text{code [eq <ICMPv6-CODE> | range <STARTING-ICMPv6-CODE> <ENDING-ICMPv6-CODE> | type [eq <ICMPV6-TYPE> | range <STARTING-ICMPV6-TYPE> <ENDING-ICMPV6-TYPE> | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}}
\]

\[
\text{permit ipv6 [any|host \langle SOURCE-HOST-IPv6 \rangle | \langle DEST-IPv6/MASK \rangle | any|host \langle DEST-HOST-IPv6 \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}}
\]

\[
\text{permit [proto | [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igp|ospf|vrrp] \langle SOURCE-IPv6/MASK \rangle | any|host \langle SOURCE-HOST-IPv6 \rangle | \langle DEST-IPv6/MASK \rangle | any|host \langle DEST-HOST-IPv6 \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}}
\]

\[
\text{permit [tcp|udp] [any|host \langle SOURCE-HOST-IPv6 \rangle | \langle DEST-IPv6/MASK \rangle | any|host \langle DEST-HOST-IPv6 \rangle | <START-PORT> <END-PORT> | \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}}
\]

Parameters

- \text{permit icmpv6 [any|host \langle SOURCE-HOST-IPv6 \rangle | \langle DEST-IPv6/MASK \rangle | any|host \langle DEST-HOST-IPv6 \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}}

| icmpv6 | Applies this permit rule to ICMPv6 packets only |
| <SOURCE-IPv6/MASK> | Specifies a range of IPv6 source address (network) to match. ICMPv6 packets received from any source in the specified network are accepted. |
| any | Specifies the source as any IPv6 address. ICMPv6 packets received from any source are accepted. |
| host \langle SOURCE-HOST-IPv6 \rangle | Identifies a specific host (as the source to match) by its IPv6 address. ICMPv6 packets received from the specified host are accepted. |
| \langle DEST-IPv6/MASK \rangle | Specifies a range of IPv6 destination address (network) to match. ICMPv6 packets addressed to any destination within the specified network are accepted. |
| any | Specifies the destination as any IPv6 address. ICMPv6 packets addressed to any destination are accepted. |
| host \langle DEST-HOST-IPv6 \rangle | Identifies a specific host (as the destination to match) by its IPv6 address. ICMPv6 packets addressed to the specified host are accepted. |
| \langle SOURCE-HOST-IPv6 \rangle | Specify the source host's exact IPv6 address. |
| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \langle START-PORT \rangle | \langle END-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-HOST-IPv6 \rangle | \langle DEST-HOST-IPv6 \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}

| \langle SOURCE-PORT \rangle | \langle DEST-PORT \rangle | \text{log,rule-precedence <1-5000> \{(rule-description \langle LINE \rangle)\}}
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<ICMPv6-TYPE>`       | Defines the ICMPv6 type field filter  
  - `eq` – Configures a specific ICMPv6 type. Specify the ICMPv6 type value.  
  - `range` – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values.  
  **Note**: ICMPv6 packets with type field value matching the values specified here are forwarded. | |
| `<ICMPv6-CODE>`       | Defines the ICMPv6 code field filter  
  - `eq` – Configures a specific ICMPv6 code. Specify the ICMPv6 code value.  
  - `range` – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values.  
  **Note**: ICMPv6 packets with code field value matching the values specified here are forwarded. | |
| `log`                 | Logs all permit events matching this entry                                                                                                                                                                  |
| `rule-precedence`     | Assigns a precedence for this permit rule  
  - `<1-5000>` – Specify a value from 1 - 5000.  
  **Note**: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. | |
| `rule-description`    | Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). | |
| `ipv6`                | Applies this permit rule to IPv6 packets only                                                                                                                                                               |
| `<SOURCE-IPv6/MASK>`  | Specifies a range of IPv6 source address (network) to match. IPv6 packets received from any source in the specified network are forwarded.                                                                  |
| `any`                 | Specifies the source as any IPv6 address. IPv6 packets received from any source are forwarded.                                                                                                              |
| `host`                | Identifies a specific host (as the source to match) by its IPv6 address. IPv6 packets received from the specified host are forwarded.  
  - `<SOURCE-HOST-IPv6>` – Specify the source host’s exact IPv6 address. | |
| `<DEST-IPv6/MASK>`    | Specifies a range of IPv6 destination address (network) to match. IPv6 packets addressed to any destination within the specified network are forwarded.                                                         |
| `any`                 | Specifies the destination as any IPv6 address. IPv6 packets addressed to any destination are forwarded.                                                                                                     |
| `host`                | Identifies a specific host (as the destination to match) by its IPv6 address. IPv6 packets addressed to the specified host are forwarded.  
  - `<DEST-HOST-IPv6>` – Specify the destination host’s exact IPv6 address. | |
| `log`                 | Logs all permit events matching this entry                                                                                                                                                                  |
| `rule-precedence`     | Assigns a precedence for this permit rule  
  - `<1-5000>` – Specify a value from 1 - 5000  
  **Note**: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. | |
<table>
<thead>
<tr>
<th>rule-description &lt;LINE&gt;</th>
<th>Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</th>
</tr>
</thead>
<tbody>
<tr>
<td>proto</td>
<td>Configures the ACL for additional protocols. Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.</td>
</tr>
<tr>
<td>&lt;PROTOCOL-NUMBER&gt;</td>
<td>Filters protocols using their Internet Assigned Numbers Authority (IANA) protocol number</td>
</tr>
<tr>
<td>• &lt;PROTOCOL-NUMBER&gt; – Specify the protocol number.</td>
<td></td>
</tr>
<tr>
<td>&lt;PROTOCOL-NAME&gt;</td>
<td>Filters protocols using their IANA protocol name</td>
</tr>
<tr>
<td>• &lt;PROTOCOL-NAME&gt; – Specify the protocol name.</td>
<td></td>
</tr>
<tr>
<td>eigrp</td>
<td>Identifies the EIGRP protocol (number 88)</td>
</tr>
<tr>
<td>EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.</td>
<td></td>
</tr>
<tr>
<td>gre</td>
<td>Identifies the GRE protocol (number 47)</td>
</tr>
<tr>
<td>GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.</td>
<td></td>
</tr>
<tr>
<td>igp</td>
<td>Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9)</td>
</tr>
<tr>
<td>IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF.</td>
<td></td>
</tr>
<tr>
<td>ospf</td>
<td>Identifies the OSPF protocol (number 89)</td>
</tr>
<tr>
<td>OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.</td>
<td></td>
</tr>
<tr>
<td>vrrp</td>
<td>Identifies the VRRP protocol (number 112)</td>
</tr>
<tr>
<td>VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.</td>
<td></td>
</tr>
<tr>
<td>&lt;SOURCE-IPv6/MASK&gt;</td>
<td>Specifies a range of IPv6 source address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source in the specified network are forwarded.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the source as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are forwarded.</td>
</tr>
</tbody>
</table>
| **host <SOURCE-HOST-IPv6>** | Identifies a specific host (as the source to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are forwarded.
| | • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address. |
| **<DEST-IPv6/MASK>** | Specifies a range of IPv6 destination address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination within the specified network are forwarded. |
| **any** | Specifies the destination as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are forwarded. |
| **host <DEST-HOST-IPv6>** | Identifies a specific host (as the destination to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified host are forwarded.
| | • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address. |
| **log** | Logs all permit events matching this entry |
| **rule-precedence <1-5000>** | Assigns a precedence for this permit rule
| | • <1-5000> – Specify a value from 1 - 5000.  
| **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. |
| **rule-description <LINE>** | Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length). |

```
host <SOURCE-HOST-IPv6>
<DEST-IPv6/MASK>   any    host <DEST-HOST-IPv6>
log                rule-precedence <1-5000>
rule-description <LINE>
tcp                udp
<source-IPv6/MASK> any
host <SOURCE-HOST-IPv6>
<source-IPv6/MASK> any
host <DEST-HOST-IPv6>
<source-IPv6/MASK> any
host <SOURCE-HOST-IPv6>
<source-IPv6/MASK> any
net <1-65535>|<SERVICE-NAME> | log,rule-precedence <1-5000> {<rule-description <LINE>}}
```

| **<SOURCE-IPv6/MASK>** | This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies a range of IPv6 source address (network) to match. TCP/UDP packets received from any source in the specified network are forwarded. |
| **any** | This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the source as any IPv6 address. TCP/UDP packets received from any source are forwarded. |
| **host <SOURCE-HOST-IPv6>** | Identifies a specific host (as the source to match) by its IPv6 address. TCP/UDP packets received from the specified host are forwarded.
| | • <SOURCE-HOST-IPv6> – Specify the source host’s exact IPv6 address. |
| **<DEST-IPv6/MASK>** | This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies a range of IPv6 destination address (network) to match. TCP/UDP packets addressed to any destination within the specified network are forwarded. |
| **any** | This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the destination as any destination IPv6 address. TCP/UDP packets received from any destination are forwarded. |
| **eq <SOURCE-PORT>** | Identifies a specific source port
| | • <SOURCE-PORT> – Specify the exact source port. |
### Examples

```bash
```

```bash
rfs7000-6DCD4B(config-ipv6-acl-test)#permit proto gre any any log rule-precedence 2
```

```bash
rfs7000-6DCD4B(config-ipv6-acl-test)#show context ipv6 access-list test
deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-command
permit proto gre any any log rule-precedence 1
```

```bash
rfs7000-6DCD4B(config-ipv6-acl-test)#
```

### Related Commands

- **no** | Removes a specified permit access rule
11.4 ip-snmp-access-list

SNMP performs network management functions using a data structure called a Management Information Base (MIB). SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.

Use SNMP ACLs to help reduce SNMP’s vulnerabilities, as SNMP traffic can be exploited to produce a denial of service (DoS).

The following table summarizes SNMP access list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a deny SNMP MIB object traffic rule</td>
<td>page 11-60</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a permit SNMP MIB object traffic rule</td>
<td>page 11-61</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny or permit SNMP MIB object traffic rule</td>
<td>page 11-62</td>
</tr>
</tbody>
</table>
11.4.1 deny

`ip-snmp-access-list`

Creates a deny SNMP MIB object traffic rule. Use this command to specify the match criteria based on which SNMP traffic is denied.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

deny [IP/M|any|host <IP>]

**Parameters**
- deny [IP/M|any|host <IP>]

| deny [IP/M|any|host <IP>] | Configures the match criteria for this deny rule
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- &lt;IP/M&gt; – Specifies a network address and mask in the A.B.C.D/M format. Packets received or destined for this network are dropped</td>
<td></td>
</tr>
<tr>
<td>- any – Specifies the match criteria as any. Packets received or destined from any address are dropped</td>
<td></td>
</tr>
<tr>
<td>- host &lt;IP&gt; – Identifies a host by its IP address. Packets received or destined for this host are dropped</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-6DCD4B(config-ip-snmp-acl-test)#deny 192.168.13.0/24
rfs7000-6DCD4B(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
deny 192.168.13.0/24
rfs7000-6DCD4B(config-ip-snmp-acl-test)#
```

**Related Commands**

| no | Removes this deny rule form the IP SNMP ACL |
11.4.2 permit

`ip-snmp-access-list`

Creates a permit SNMP MIB object traffic rule. Use this command to specify the match criteria based on which SNMP traffic is permitted.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
permit [IP/M|any|host <IP>]
```

Parameters

- `permit [IP/M|any|host <IP>]`

| `permit [IP/M|any|host <IP>]` | Configures the match criteria for this permit rule |
|-------------------------------|-----------------------------------------------|
| `IP/M`                        | Specifies a network address and mask in the A.B.C.D/M format. Packets received or destined for this network are forwarded |
| `any`                         | Specifies the match criteria as any. Packets received or destined from any address are forwarded |
| `host <IP>`                   | Identifies a host by its IP address. Packets received or destined for this host are forwarded |

Examples

```
rfs7000-6DCD4B(config-ip-snmp-acl-test)#permit host 192.168.13.13
rfs7000-6DCD4B(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
   permit host 192.168.13.13
deny 192.168.13.0/24
rfs7000-6DCD4B(config-ip-snmp-acl-test)#
```

Related Commands

```
no
```

Removes this permit rule form the IP SNMP ACL
11.4.3 no

ip-snmp-access-list

Removes a deny or permit rule from the IP SNMP ACL. Use this command to remove IP SNMP ACL as they become obsolete for filtering network access permissions.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|permit] [<IP/M>|any|host <IP>]

Parameters

- no <PARAMETERS>

no <PARAMETERS> Removes deny and/or permit access rule from this IP SNMP ACL

Examples

rfs7000-6DCD4B(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
  permit host 192.168.13.13
  deny 192.168.13.0/24
rfs7000-6DCD4B(config-ip-snmp-acl-test)#

rfs7000-6DCD4B(config-ip-snmp-acl-test)#no permit host 192.168.13.13

rfs7000-6DCD4B(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
  deny 192.168.13.0/24
rfs7000-6DCD4B(config-ip-snmp-acl-test)#
11.5 ex3500-ext-access-list

IP ACLs function as firewalls that filter or mark packets on layer 3 ports as opposed to MAC ACLs that filter traffic on layer 2 ports.

An IPv4 EX3500 extended ACL is a policy-based ACL that either prevents or allows specific clients from using the EX3500 switch. It allows you to permit or deny client access by specifying that the traffic from a specific host or network and/or the traffic to a specific host or network be either denied or permitted.

An EX3500 extended ACL consists of a set of deny /permit rules that filter packets based on both source and destination IPv4 addresses. Each rule specifies a set of match criteria (the source and destination IP addresses) and has a unique precedence value assigned. These ACL rules are applied sequentially to the traffic at a port, by a firewall-supported device, in an increasing order of their precedence. When a packet matches the criteria specified in a rule the packet is either forwarded or dropped based on the rule type.

The following table summarizes IPv4 EX3500 extended ACL configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined to specified address(es).</td>
<td>page 11-64</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined to specified address(es).</td>
<td>page 11-67</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny and/or a permit access rule from this IPv4 EX3500 extended ACL</td>
<td>page 11-70</td>
</tr>
</tbody>
</table>

NOTE: To implement the EX3500 extended ACL, apply it directly to a EX3500 device, or to an EX35XX profile. For more information see, access-group.
11.5.1 deny

Creates a deny ACL rule that filters packets based on the source and/or destination IPv4 address, and other specified criteria. You can also use this command to modify an existing deny rule.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

Syntax

```
deny [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] [<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>] [destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>] [ex3500-time-range <TIME-RANGE-NAME>|ip-precedence <0-63]|rule-precedence <1-128> [source-port <0-65535]|source-port-bitmark <0-65535>
```

Parameters

- **deny [<0-255]|tcp|udp]** Creates a deny rule and identifies the protocol type. This deny rule is applied only to packets matching the protocol specified here.
  - `<0-255>` – Identifies the protocol from its number. Specify the protocol number from 0 - 255.
  - `tcp` – Configures the protocol as TCP
  - `udp` – Configures the protocol as UDP

- **<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>** Specifies the source IP address as any, host, or network
  - `<SOURCE-NETWORK-IP/MASK>` – Configures a network as the source. Provide the network’s IPv4 address along with the mask.
  - `host <SOURCE-HOST-IP>` – Configures a single device as the source. Provide the host device’s IPv4 address.
  - `any` – Specifies that the source can be any device

- **<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>** Specifies the destination IP address as any, host, or network.
  - `<DEST-NETWORK-IP/MASK>` – Configures a network as the destination. Provide the network’s IPv4 address along with the mask.
  - `host <DEST-HOST-IP>` – Configures a single device as the destination. Provide the host device’s IPv4 address.
  - `any` – Specifies that the destination can be any device

- **control-flag <0-63>** Configures the decimal number (representing a bit string) that specifies the control flag bits in byte 14 of the TCP header
  - `<0-63>` – Specify a value from 0 - 63.

**Note:** Control flags can be used only in ACLs designed to filter TCP traffic. The TCP header contains several one-bit boolean fields known as flags that influence flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags.
- URG flag - Marks incoming packet as urgent. Contd...
**Usage Guidelines**

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- TCP
- UDP
- <0-255> (any Internet protocol other than TCP, UDP, and ICMP)

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria
Examples
The following example denies TCP outgoing packets from all sources within the 192.168.14.0 network to a specific host 192.168.13.13:

rule-precedence 1#

nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#

Related Commands

| no | Removes a specified deny access rule from this IPv4 EX3500 extended ACL |
11.5.2 permit

*ex3500-ext-access-list*

Creates a permit ACL rule that filters packets based on the source and/or destination IPv4 address, and other specified criteria. You can also use this command to modify an existing permit rule.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

```
permit [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>]
[control-flag <0-63>]
destination-port <0-65535> destination-port-bitmark <0-65535> dscp <0-63>
ex3500-time-range <TIME-RANGE-NAME> ip-precedence <0-63> rule-precedence <1-128>
sourcestate <0-65535> source-port-bitmark <0-65535>
```

**Parameters**

- `permit [<0-255]|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
  [DEST-NETWORK-IP/MASK|any|host <DEST-HOST-IP>]
  [control-flag <0-63>]
destination-port <0-65535> destination-port-bitmark <0-65535> dscp <0-63>
ex3500-time-range <TIME-RANGE-NAME> ip-precedence <0-63> rule-precedence <1-128>
sourcestate <0-65535> source-port-bitmark <0-65535>`

**permit [0-255] | tcp | udp**

- Creates a permit rule and identifies the protocol type. This permit rule is applied only to packets matching the protocol specified here.
  - `<0-255>` – Identifies the protocol from its number. Specify the protocol number from 0 - 255.
  - `tcp` – Configures the protocol as TCP
  - `udp` – Configures the protocol as UDP

**[<SOURCE-NETWORK-IP/MASK>] | any | host <SOURCE-HOST-IP>**

- Specifies the source IP address as *any*, *host*, or *network*.
  - `<SOURCE-NETWORK-IP/MASK>` – Configures a network as the source. Provide the network’s IPv4 address along with the mask.
  - `host <SOURCE-HOST-IP>` – Configures a single device as the source. Provide the host device’s IPv4 address.
  - `any` – Specifies that the source can be any device

**[<DEST-NETWORK-IP/MASK>] | any | host <DEST-HOST-IP>**

- Specifies the destination IP address as *any*, *host*, or *network*.
  - `<DEST-NETWORK-IP/MASK>` – Configures a network as the destination. Provide the network’s IPv4 address along with the mask.
  - `host <DEST-HOST-IP>` – Configures a single device as the destination. Provide the host device’s IPv4 address.
  - `any` – Specifies that the destination can be any device

**control-flag <0-63>**

- Configures the decimal number (representing a bit string) that specifies the control flag bits in byte 14 of the TCP header
  - `<0-63>` – Specify a value from 0 - 63.

**Note:** Control flags can be used only in ACLs designed to filter TCP traffic. The TCP header contains several one-bit boolean fields known as flags that influence flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags.
  - URG flag - Marks incoming packet as urgent.
  - Contd...
**Usage Guidelines**

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- TCP
- UDP
- <0-255> (any Internet protocol other than TCP, UDP, and ICMP)

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination-port</strong></td>
<td>Configures the protocol destination port to match. The destination protocol can be TCP, UDP or any other protocol identified by its number (&lt;0-255&gt;).</td>
</tr>
<tr>
<td>&lt;0-65535&gt;</td>
<td>- Specify the destination port from 0 - 65535.</td>
</tr>
<tr>
<td><strong>destination-port-bitmark</strong></td>
<td>Configures the decimal number representing the protocol destination port bits to match</td>
</tr>
<tr>
<td>&lt;0-65535&gt;</td>
<td>- Specify the destination port bits from 0 - 65535.</td>
</tr>
<tr>
<td><strong>dscp</strong></td>
<td>Configures the DSCP priority level</td>
</tr>
<tr>
<td>&lt;0-63&gt;</td>
<td>- Specify a value from 0 - 63.</td>
</tr>
<tr>
<td><strong>ex3500-time-range</strong></td>
<td>Applies a periodic or absolute time range to this rule</td>
</tr>
<tr>
<td>&lt;TIME-RANGE-NAME&gt;</td>
<td>- Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see <a href="#">ex3500</a>.</td>
</tr>
<tr>
<td><strong>ip-precedence</strong></td>
<td>Configures the IP header precedence</td>
</tr>
<tr>
<td>&lt;0-7&gt;</td>
<td>- Specify a value from 0 - 7.</td>
</tr>
<tr>
<td><strong>source-port</strong></td>
<td>Configures the protocol source port to match. The source protocol can be TCP, UDP or any other protocol identified by its number (&lt;0-255&gt;).</td>
</tr>
<tr>
<td>&lt;0-65535&gt;</td>
<td>- Specify the source port from 0 - 65535.</td>
</tr>
<tr>
<td><strong>source-port-bitmark</strong></td>
<td>Configures the decimal number representing the protocol source port bits to match</td>
</tr>
<tr>
<td>&lt;0-65535&gt;</td>
<td>- Specify the source port bits from 0 - 65535.</td>
</tr>
<tr>
<td><strong>rule-precedence</strong></td>
<td>The following keywords are recursive and common to all of the above parameters:</td>
</tr>
<tr>
<td>&lt;1-128&gt;</td>
<td>- rule-precedence – Assigns a precedence to this permit rule</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-128&gt; – Specify a value from 1 - 5000.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 4 and is applied first to packets.</td>
</tr>
</tbody>
</table>
**Examples**
The following example permits outgoing TCP packets from all sources within the 192.168.14.0 network to any destination, with the TCP control flag set to 16 (acknowledge):

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
```

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context ip ex3500-ext-access-list test
deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a specified permit access rule from this IPv4 EX3500 extended ACL</td>
</tr>
</tbody>
</table>
11.5.3 no

`ex3500-ext-access-list`

Removes a deny or permit access rule from this IPv4 EX3500 extended ACL

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

```
no [deny|permit] [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>]
destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>
ex3500-time-range <TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>
source-port <0-65535>|source-port-bitmark <0-65535>
```

**Parameters**
- no <PARAMETERS>

**Usage Guidelines**

The keyword ‘control-flag <0-63>’ is only applicable to ACL rules filtering TCP traffic.

**Examples**

The following example shows the IPv4 EX3500 extended ACL ‘test’ settings before the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
```

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

The following example shows the IPv4 EX3500 extended ACL ‘test’ settings after the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
```

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```
11.6 ex3500-std-access-list

A EX3500 standard ACL is a policy-based ACL that contains a set of filter criteria and action that is applied to traffic originating from a specified source.

The following table summarizes IPv4 EX3500 standard ACL configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a deny rule that rejects packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing deny rule.</td>
<td>page 11-72</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a permit rule that allows packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing permit rule.</td>
<td>page 11-73</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny and/or a permit access rule from this IPv4 EX3500 extended ACL</td>
<td>page 11-74</td>
</tr>
</tbody>
</table>

**NOTE:** To implement the EX3500 standard ACL, apply it directly to a EX3500 device, or to an EX35XX profile. For more information see, access-group.
11.6.1 deny

`ex3500-std-access-list`

Creates a deny rule that rejects packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing deny rule.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

deny [<SOURCE-NETWORK-IP/MASK> | any | host <SOURCE-HOST-IP>] {ex3500-time-range <TIME-RANGE-NAME>}

**Parameters**

- deny [<SOURCE-NETWORK-IP/MASK> | any | host <SOURCE-HOST-IP>] {ex3500-time-range <TIME-RANGE-NAME>}
  - Creates a deny rule that rejects packets from a specified source or a network. Use one of the following options to specify the source: any, host, or network.
  - `<SOURCE-NETWORK-IP/MASK>` – Configures a network as the source. Provide the network's IPv4 address along with the mask.
  - host `<SOURCE-HOST-IP>` – Configures a single device as the source. Provide the host device's IPv4 address.
  - any – Specifies that the source can be any device

- ex3500-time-range <TIME-RANGE-NAME>
  - Optional. Applies a periodic or absolute time range to this deny rule
    - `<TIME-RANGE-NAME>` – Specify the time range name (should be existing and configured). The ACL is triggered during the time period configured in the specified EX3500 time range. For information on configuring EX3500 time-range, see `ex3500`.

**Examples**

nx9500-6C8809(config-ip-ex3500-std-acl-test)#deny 192.168.14.0/24

nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
deny 192.168.13.0/24

nx9500-6C8809(config-ip-ex3500-std-acl-test)#

**Related Commands**

- `no` Removes a specified deny access rule from this IPv4 EX3500 standard ACL
11.6.2 permit

**ex3500-std-access-list**

Creates a permit rule that allows packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing permit rule.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

```
permit [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
{ex3500-time-range <TIME-RANGE-NAME>}
```

**Parameters**

- `permit [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]` creates a permit rule that allows packets from a specified source or a network. Use one of the following options to specify the source:
  - `any` — Specifies that the source can be any device.
  - `host <SOURCE-HOST-IP>` — Configures a single device as the source. Provide the host device’s IPv4 address.
  - `<SOURCE-NETWORK-IP/MASK>` — Configures a network as the source. Provide the network's IPv4 address along with the mask.

- `ex3500-time-range <TIME-RANGE-NAME>` — Applies a periodic or absolute time range to this deny rule. Specify the time range name (should be existing and configured). The ACL is triggered during the time period configured in the specified EX3500 time range. For information on configuring EX3500 time-range, see **ex3500**.

**Examples**

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01

nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
deny 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
```

**Related Commands**

- `no` Removes a specified permit access rule from this IPv4 EX3500 standard ACL
11.6.3 no

*ex3500-std-access-list*

Removes a deny or permit access rule from this IPv4 EX3500 standard ACL

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

no [deny|permit] [<SOURCE-IP/MASK>|any|host <IP>] {ex3500-time-range <TIME-RANGE-NAME>}

**Parameters**

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Removes a deny or permit access rule based on the parameters passed</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the IPv4 EX3500 standard ACL ‘test’ settings before the ‘no’ commands are executed:

nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context ip ex3500-std-access-list test
  deny 192.168.14.0/24
  permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#

nx9500-6C8809(config-ip-ex3500-std-acl-test)#no deny 192.168.14.0/24

The following example shows the IPv4 EX3500 standard ACL ‘test’ settings after the ‘no’ commands are executed:

nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context ip ex3500-std-access-list test
  permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
CHAPTER 12
DHCP-SERVER-POLICY

This chapter summarizes Dynamic Host Control Protocol (DHCP) server policy commands in the CLI command structure.

DHCP automatically assigns network IP addresses to requesting clients to enable them access to network resources. DHCP tracks IP address assignments, their lease times and their availability. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the controller's (wireless controller, service platform, or access point) onboard DHCP server allocates an address to a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, wireless clients (with assigned leases) are expected to renew them to continue using the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The controller's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). IP address management is conducted by a controller's DHCP server and not by an administrator.

The controller's internal DHCP server groups wireless clients based on defined user-class options. Clients with a defined set of user-class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnets. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Use the (config) instance to configure DHCP/DHCPv6 server policy parameters. To navigate to the config DHCP server policy instance, use the following commands:

```text
<DEVICE>(config)#dhcp-server-policy <POLICY-NAME>
```

```text
rfs7000-37FABE(config)#dhcp-server-policy test
rfs7000-37FABE(config-dhcp-server-policy-test)#
```

```text
rfs7000-37FABE(config-dhcp-policy-test-2)#
```

DHCP policy Mode commands:

- bootp: BOOTP specific configuration
- dhcp-class: Configure DHCP class (for address allocation using DHCP user-class options)
- dhcp-pool: Configure DHCP server address pool
- dhcp-server: Activating dhcp server based on criteria
- no: Negate a command or set its defaults
- option: Define DHCP server option
- ping: Specify ping parameters used by DHCP Server
- clrscr: Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
drop End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test)#

To navigate to the config DHCPv6 server policy instance, use the following commands:
<DEVICE>(config)#dhcpv6-server-policy <POLICY-NAME>

rfs7000-37FABE(config)#dhcpv6-server-policy test
rfs7000-37FABE(config-dhcpv6-server-policy-test)#

rfs7000-37FABE(config-dhcpv6-server-policy-test)#?
DHCPv6 server policy Mode commands:
dhcpv6-pool Configure DHCPV6 server address pool
no Negate a command or set its defaults
option Define DHCPV6 server option
restrict-vendor-options Restrict vendor specific options to be sent in
server reply
server-preference Server preference value sent in the reply, by the
server to client

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
drop End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcpv6-server-policy-test)#

This chapter is organized as follows:

• dhcp-server-policy
• dhcpv6-server-policy

----

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across
this chapter, cannot include an underscore (_) character. In other words, the
name of a device cannot contain an underscore.
12.1 dhcp-server-policy

The following table summarizes DHCP server policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootp</td>
<td>Configures a BOOTP specific configuration</td>
<td>page 12-4</td>
</tr>
<tr>
<td>dhcp-class</td>
<td>Configures a DHCP server class</td>
<td>page 12-5</td>
</tr>
<tr>
<td>dhcp-pool</td>
<td>Configures a DHCP server address pool</td>
<td>page 12-11</td>
</tr>
<tr>
<td>dhcp-server</td>
<td>Configures the activation-criteria that triggers dynamic activation of DHCP service running on a redundancy device</td>
<td>page 12-54</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 12-56</td>
</tr>
<tr>
<td>option</td>
<td>Defines the DHCP option used in DHCP pools</td>
<td>page 12-57</td>
</tr>
<tr>
<td>ping</td>
<td>Specifies ping parameters used by a DHCP server</td>
<td>page 12-58</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *Chapter 5, COMMON COMMANDS.*
12.1.1 **bootp**

- **dhcp-server-policy**

Configures a BOOTP specific configuration

*Bootstrap Protocol* (BOOTP) requests are used by UNIX diskless workstations to obtain the location of their boot image and IP address within the managed network. A BOOTP configuration server provides this information and also assigns an IP address from a configured pool of IP addresses. By default, all BOOTP requests are forwarded to the BOOTP configuration server by the controller. When enabled, this feature allows controllers, using this DHCP server policy, to ignore BOOTP requests.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

bootp ignore

**Parameters**

- bootp ignore

<table>
<thead>
<tr>
<th>bootp ignore</th>
<th>Enables controllers to ignore BOOTP requests</th>
</tr>
</thead>
</table>

**Examples**

rfs7000-37FABE(config-dhcp-policy-test)#bootp ignore

rfs7000-37FABE(config-dhcp-policy-test)#show context dhcp-server-policy test
  bootp ignore
rfs7000-37FABE(config-dhcp-policy-test)#

**Related Commands**

- **no** Disables the ignore BOOTP requests option
12.1.2 dhcp-class

A controller, service platform, or access point’s local DHCP server assigns IP addresses to requesting DHCP clients based on user class option names. The DHCP server can assign IP addresses from as many IP address ranges as defined by an administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

A DHCP user class applies different DHCP settings to a set of wireless clients. Wireless clients using the same DHCP settings are grouped under one DHCP class. Grouping users into classes facilitates the provision of differentiated service.

The following table summarizes DHCP class configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-class</td>
<td>Creates a DHCP class and enters its configuration mode</td>
<td>page 12-6</td>
</tr>
<tr>
<td>dhcp-class-mode</td>
<td>Invokes DHCP class configuration commands</td>
<td>page 12-7</td>
</tr>
<tr>
<td>commands</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
12.1.2.1 dhcp-class

Creates a DHCP server class and enters its configuration mode. Use this command to configure user class option values. Once defined, the controller’s internal DHCP server uses the configured values to group wireless clients into DHCP classes. Therefore, each user class consists of wireless clients sharing the same set of user class values.

You can also use this command to modify an existing DHCP user class settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-class <DHCP-CLASS-NAME>

Parameters
- dhcp-class <DHCP-CLASS-NAME>

Examples

rfs7000-37FABE(config-dhcp-policy-test)#dhcp-class dhcpclass1

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#?

DHCP class Mode commands:
- multiple-user-class Enable multiple user class option
- no Negate a command or set its defaults
- option Configure DHCP Server options
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#

Related Commands

no Removes a configured DHCP user class policy
12.1.2.2 dhcp-class-mode commands

- dhcp-class

Use DHCP class mode commands to configure the parameters of the DHCP user class.

The following table summarizes DHCP user class configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiple-user-class</td>
<td>Enables multiple user class option for this DHCP user class policy</td>
<td>page 12-8</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 12-9</td>
</tr>
<tr>
<td>option</td>
<td>Configures DHCP user class options for this DHCP user class policy</td>
<td>page 12-10</td>
</tr>
</tbody>
</table>
12.1.2.2.1 multiple-user-class

*dhcp-class-mode commands*

Enables multiple user class option for this DHCP user class policy. Enabling this option allows this user class to transmit multiple option values to other DHCP servers also supporting multiple user class options.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
multiple-user-class
```

**Parameters**

None

**Examples**

```plaintext
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#multiple-user-class

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
  **multiple-user-class**

rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables the multiple user class option for the selected DHCP user class policy</td>
</tr>
</tbody>
</table>
12.1.2.2 no

- **dhcp-class-mode commands**

Removes this DHCP user class policy's settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [multiple-user-class|option]
no option user-class <VALUE>
```

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Disables multiple user class options on this DHCP user class policy |

**Examples**

The following example shows the DHCP class settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
  option user-class hex
  multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

```
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#no multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#no option user-class hex
```

The following example shows the DHCP class settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```
12.1.2.2.3 option

`dhcp-class-mode commands`

Configures DHCP user class options for this DHCP user class policy

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`option user-class <VALUE>`

Parameters

- `option user-class <VALUE>`

Examples

```
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#option user-class hex
```
```
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
  option user-class hex
  multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands

```
no
```

Removes the configured DHCP user class option
12.1.3 dhcp-pool

The DHCP pool command creates and manages a pool of IP addresses. These IP addresses are assigned to devices using the DHCP protocol. IP addresses have to be unique for each device in the network. Since IP addresses are finite, DHCP ensures that every device, in the network, is issued a unique IP address by tracking the issue, release, and reissue of IP addresses.

The DHCP pool command configures a finite set of IP addresses that can be assigned whenever a device joins a network.

The following table summarizes DHCP pool configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-pool</td>
<td>Creates a DHCP pool and enters its configuration mode</td>
<td>page 12-12</td>
</tr>
<tr>
<td>dhcp-pool-mode</td>
<td>Summarizes DHCP pool configuration mode commands</td>
<td>page 12-14</td>
</tr>
</tbody>
</table>
12.1.3.1 dhcp-pool

Configures a DHCP server address pool

DHCP services are available for specific IP interfaces. A pool (or range) of IP network addresses and DHCP options can be created for each IP interface defined. This range of addresses is available to DHCP enabled wireless devices on either a permanent or leased basis. This enables the reuse of limited IP address resources for deployment in any network. DHCP options are provided to each DHCP client with a DHCP response and provides DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCP client.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-pool <POOL-NAME>

Parameters
- dhcp-pool <POOL-NAME>

Examples

rfs7000-37FABE(config-dhcp-policy-test)#dhcp-pool pool1

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#?

DHCP pool Mode commands:
- address: Configure network pool's included addresses
- bootfile: Boot file name
- ddns: Dynamic DNS Configuration
- default-router: Default routers
- dns-server: DNS Servers
- domain-name: Configure domain-name
- excluded-address: Prevent DHCP Server from assigning certain addresses
- lease: Address lease time
- netbios-name-server: NetBIOS (WINS) name servers
- netbios-node-type: NetBIOS node type
- network: Network on which DHCP server will be deployed
- next-server: Next server in boot process
- no: Negate a command or set its defaults
- option: Raw DHCP options
- respond-via-unicast: Send DHCP offer and DHCP Ack as unicast messages
- static-binding: Configure static address bindings
- static-route: Add static routes to be installed on dhcp clients
- update: Control the usage of DDNS service

clrscr: Clears the display screen
commit: Commit all changes made in this session
do: Run commands from Exec mode
end: End current mode and change to EXEC mode
exit: End current mode and down to previous mode
help                  Description of the interactive help system
revert                Revert changes
service               Service Commands
show                  Show running system information
write                 Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes a specified DHCP address pool</td>
</tr>
</tbody>
</table>
12.1.3.2 dhcp-pool-mode commands

- **dhcp-pool**

  Configures the DHCP pool parameters

The following table summarizes DHCP pool configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Specifies a range of addresses for a DHCP address pool</td>
<td>page 12-15</td>
</tr>
<tr>
<td>bootfile</td>
<td>Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.</td>
<td>page 12-17</td>
</tr>
<tr>
<td>ddns</td>
<td>Configures dynamic DNS parameters</td>
<td>page 12-18</td>
</tr>
<tr>
<td>default-router</td>
<td>Configures a default router or gateway IP address for the network pool</td>
<td>page 12-20</td>
</tr>
<tr>
<td>dns-server</td>
<td>Sets a DNS server’s IP address available to all DHCP clients connected to the DHCP pool</td>
<td>page 12-21</td>
</tr>
<tr>
<td>domain-name</td>
<td>Sets the domain name for the network pool</td>
<td>page 12-23</td>
</tr>
<tr>
<td>excluded-address</td>
<td>Prevents a DHCP server from assigning certain addresses to the DHCP pool</td>
<td>page 12-24</td>
</tr>
<tr>
<td>lease</td>
<td>Sets a valid lease for the IP address used by DHCP clients in the DHCP pool</td>
<td>page 12-26</td>
</tr>
<tr>
<td>netbios-name-server</td>
<td>Configures a NetBIOS (WINS) name server’s IP address</td>
<td>page 12-27</td>
</tr>
<tr>
<td>netbios-node-type</td>
<td>Defines the NetBIOS node type</td>
<td>page 12-28</td>
</tr>
<tr>
<td>network</td>
<td>Configures the network on which the DHCP server is deployed</td>
<td>page 12-29</td>
</tr>
<tr>
<td>next-server</td>
<td>Configures the next server in the boot process</td>
<td>page 12-30</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 12-9</td>
</tr>
<tr>
<td>option</td>
<td>Configures RAW DHCP options</td>
<td>page 12-10</td>
</tr>
<tr>
<td>respond-via-unicast</td>
<td>Sends a DHCP offer and DHCP Ack as unicast messages</td>
<td>page 12-35</td>
</tr>
<tr>
<td>static-route</td>
<td>Configures a static route for a DHCP pool</td>
<td>page 12-34</td>
</tr>
<tr>
<td>update</td>
<td>Controls the usage of the DDNS service</td>
<td>page 12-36</td>
</tr>
<tr>
<td>static-binding</td>
<td>Configures static address bindings</td>
<td>page 12-37</td>
</tr>
</tbody>
</table>
12.1.3.2.4 address

**dhcp-pool-mode commands**

Adds IP addresses to the DHCP address pool. These IP addresses are assigned to each device joining the network.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
address [<IP>|<HOST-ALIAS-NAME>|range]
```

**Parameters**
- `address [<IP>|<HOST-ALIAS-NAME>|range]` Adds a single IP address to the DHCP address pool.
- `<IP>` Adds a single IP address to the DHCP address pool.
- `<HOST-ALIAS-NAME>` Adds a single host mapped to the specified host alias. The host alias should be existing and configured.
  - **Note:** A network host alias maps a name to a single network host. For example, `alias host $HOST 1.1.1.100`. In this example the host alias is `$HOST` and it maps to a single host `1.1.1.100`. For more information, see `alias`.
- `range [START-IP]<START-HOST-ALIAS-NAME>] [END-IP]<END-HOST-ALIAS-NAME>]` Adds a range of IP addresses to the DHCP address pool. Use one of the following options to provide the first IP address in the range:
  - `START-IP` – Specifies the first IP address in the range
  - `START-HOST-ALIAS-NAME` – Specifies a host alias, mapped to the first IP address in the range
  - `END-IP` – Specifies the last IP address in the range
  - `END-HOST-ALIAS-NAME` – Specifies a host alias, mapped to the last IP address in the range
  - **Note:** The host aliases should be existing and configured.
- `class <DHCP-CLASS-NAME>` Optional. Applies additional DHCP options, or a modified set of options to those available to wireless clients. For more information, see `dhcp-class`.
  - `<DHCP-CLASS-NAME>` – Sets the DHCP class.

**Examples**

```plaintext
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#address 192.168.13.4 class dhcpclass1
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
   address 192.168.13.4 class dhcpclass1
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the DHCP pool’s configured IP addresses</td>
</tr>
<tr>
<td><code>dhcp-class</code></td>
<td>Creates and configures the DHCP class parameters</td>
</tr>
<tr>
<td><code>alias</code></td>
<td>Creates and configures a network, VLAN, host, string, and network-service aliases</td>
</tr>
</tbody>
</table>
12.1.3.2.5 bootfile

*dhcp-pool-mode commands*

The Bootfile command provides a diskless node path to the image file while booting up. Only one file can be configured for each DHCP pool.

For more information on the BOOTP protocol with reference to the DHCP policy, see *bootp*.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
bootfile <IMAGE-FILE-PATH>
```

**Parameters**

- `bootfile <IMAGE-FILE-PATH>`

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets the boot image path for BOOTP clients</td>
</tr>
<tr>
<td><code>bootp</code></td>
<td>Configures BOOTP protocol parameters</td>
</tr>
</tbody>
</table>
12.1.3.2.6 ddns

 dhcp-pool-mode commands

Configures Dynamic Domain Name Service (DDNS) parameters. Dynamic DNS provides a way to access an individual device in a DHCP serviced network using a static device name. Depending on the DHCP server’s configuration, the IP address of a device changes periodically. To ensure continuous accessibility to a device (having a dynamic IP address), the device’s current IP address is published to a DDNS server that resolves the static device name (used to access the device) with a changing IP address. The DDNS server must be accessible from outside the network and must be configured as an address resolver. Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ddns [domainname|multiple-user-class|server|ttl]
ddns domainname <DDNS-DOMAIN-NAME>
ddns multiple-user-class
ddns server [<IP>|<HOST-ALIAS-NAME>]{<IP1>|<HOST-ALIAS-NAME1>}
ddns ttl <1-864000>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domainname</td>
<td>&lt;DDNS-DOMAIN-NAME&gt; Sets the domain name used for DNS updates</td>
</tr>
<tr>
<td>multiple-user-class</td>
<td>Enables the multiple user class options with this DDNS domain</td>
</tr>
<tr>
<td>server</td>
<td>Configures the DDNS server used by this DHCP profile</td>
</tr>
</tbody>
</table>

- **domainname**: Sets the domain name used for DNS updates. The controller uses DNS to convert human readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A Fully Qualified Domain Name (FQDN) consists of a host name plus a domain name. For example, computername.domain.com.

- **multiple-user-class**: Enables the multiple user class options with this DDNS domain.

- **server**: Configures the primary DDNS server. This is the default server. Use one of the following options to specify the primary DDNS server:
  - <IP> – Specifies the primary DDNS server’s IP address
  - <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DDNS server’s IP address. The host alias should be existing and configured.

**Note**: A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see alias.
## ddns ttl <1-864000>

<table>
<thead>
<tr>
<th></th>
<th>Optional. Configures the secondary DDNS server. If the primary server is not reachable, this server is used. Use one of the following options to identify the secondary DDNS server:</th>
</tr>
</thead>
</table>
| `{<IP1>|<HOST-ALIAS-NAME1>}` | • `<IP>` – Specifies the secondary DDNS server’s IP address  
  • `<HOST-ALIAS-NAME>` – Specifies a host alias, mapped to the secondary DDNS server’s IP address. The host alias should be existing and configured. |
| `ttl <1-864000>` | Configures the *Time To Live* (TTL) value for DDNS updates  
  • `<1-86400>` – Specify a value from 1- 864000 seconds. |

### Examples

```plaintext
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns domainname WID
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns multiple-user-class
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns server 192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
    address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns domainname WID
ddns multiple-user-class
bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

| `no` | Resets or disables a DHCP pool’s DDNS settings |
12.1.3.2.7 default-router

- **dhcp-pool-mode commands**

  Configures a default router or gateway IP address for a network pool

After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address of one or a group of routers the controller uses to map host names into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

**Parameters**

```
  default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
  
  [<IP>|<HOST-ALIAS-NAME>] Configures the primary default router, using one of the following options:
  • <IP> – Specifies the primary default router’s IP address
  • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router’s IP address

  {<IP1>|<HOST-ALIAS-NAME1>} Optional. Configures the secondary default router, using one of the following options:
  • <IP1> – Specifies the secondary default router’s IP address
  • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary default router’s IP address. If the primary default router is unavailable, the secondary router is used.

  **Note:** A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see alias.

  **Note:** A maximum of 8 default routers can be configured.
```

**Usage Guidelines**

The IP address of the router should be on the same subnet as the client subnet.

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#default-router 192.168.13.8 192.168.13.9

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns domainname WID
ddns multiple-user-class
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

**Related Commands**

```
  no Removes the default router settings
```
12.1.3.2.8 dns-server

`dhcp-pool-mode commands`

Configures a network’s DNS server. The DNS server supports all clients connected to networks supported by the DHCP server.

For DHCP clients, the DNS server’s IP address maps the hostname to an IP address. DHCP clients use the DNS server’s IP address based on the order (sequence) configured.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}

**Parameters**
- dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1> <HOST-ALIAS-NAME1>}

<table>
<thead>
<tr>
<th>[&lt;IP&gt;] &lt;HOST-ALIAS-NAME&gt;</th>
<th>Configures the primary DNS server, using one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt; – Specifies the primary DNS server’s IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary DNS server’s IP address</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** A maximum of 8 DNS servers can be configured.

**Note:** To enable redirection of DSN queries to OpenDNS it is necessary that the DNS server IP address provided here should point to the OpenDNS IP address. OpenDNS is a proxy DNS server that provides additional functionality, such as Web filtering, reporting, and performance enhancements. When configured on a WLAN, DNS queries from wireless clients are redirected to OpenDNS. For more information on configuring OpenDNS on a WLAN, see `opendns`.

| {<IP1>|<HOST-ALIAS-NAME1>} | Optional. Configures the secondary DNS server, using one of the following options: |
|--------------------------|--------------------------------------------------------------------------------------------|
| <IP1> – Specifies the secondary DNS server’s IP address |
| <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary DNS server’s IP address. If the primary DNS server is unavailable, the secondary server is used. |

**Note:** A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see `alias`.

**Note:** A maximum of 8 DNS servers can be configured.

**Examples**

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#dns-server 192.168.13.19

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns domainname WID
ddns multiple-user-class
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes DNS server settings</td>
</tr>
</tbody>
</table>
12.1.3.2.9 domain-name

Sets the domain name for the DHCP pool. This is the domain name used by the controller with this pool. Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. The FQDN consists of the host name and the domain name. For example, computernamespace.domain.com.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
domain-name <DOMAIN-NAME>

Parameters
- domain-name <DOMAIN-NAME>

Examples
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#domain-name documentation
dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
dns server 192.168.13.9
dns domainname WID
dns multiple-user-class
domain-name documentation
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

Related Commands
- no
  Removes a DHCP pool’s domain name
12.1.3.2.10 excluded-address

Identifies a single IP address or a range of IP addresses, included in the DHCP address pool, that cannot be assigned to clients by the DHCP server.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

excluded-address [<IP>|<HOST-ALIAS-NAME>|range]
excluded-address <IP>
excluded-address <HOST-ALIAS-NAME>
excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]

Parameters

- **excluded-address <IP>**
  Adds a single IP address to the excluded address list

- **excluded-address <HOST-ALIAS-NAME>**
  Adds a host alias. The host alias is mapped to a host’s IP address. The host identified by the host alias is added to the excluded address list. The host alias should be existing and configured.
  **Note:** A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is `$HOST` and it maps to a single host ‘1.1.1.100’. For more information, see alias.

- **excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]**
  Adds a range of IP addresses to the excluded address list. Use one of the following options to provide the first IP address in the range:
  - `<START-IP>` — Specifies the first IP address in the range
  - `<START-HOST-ALIAS-NAME>` — Specifies a host alias, mapped to the first IP address in the range
  Use one of the following options to provide the last IP address in the range:
  - `<END-IP>` — Specifies the last IP address in the range
  - `<END-HOST-ALIAS-NAME>` — Specifies a host alias, mapped to the last IP address in the range
  **Note:** The host aliases should be existing and configured.
Examples

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#excluded-address range 192.168.13.25 192.168.13.28

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns domainname WID
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the exclude IP addresses settings</td>
</tr>
</tbody>
</table>
12.1.3.2.11 lease

A lease is the duration a DHCP issued IP address is valid. Once a lease expires, and if the lease is not renewed, the IP address is revoked and is available for reuse. Generally, before an IP lease expires, the client tries to get the same IP address issued for the next lease period. This feature is enabled by default, with a lease period of 24 hours (1 day).

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
lease [0-365]|infinite]

lease <0-365> {0-23} {0-59} {0-59}
```

Parameters

- `infinite`: The lease never expires (equal to a static IP address assignment)
- `lease <0-365> {0-23} {0-59} {0-59}`

Usage Guidelines

If lease parameter is not configured on the DHCP pool, the default is used. The default is 24 hours.

Examples

```plaintext
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#lease 100 23 59 59

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  dns_server 192.168.13.9
  dns_domainname WID
  dns_multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

- `no`: Resets values or disables the DHCP pool lease settings
**12.1.3.2.12 netbios-name-server**

* dhcp-pool-mode commands

Configures the NetBIOS (WINS) name server’s IP address. This server is used to resolve NetBIOS host names. Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

**Parameters**

- `netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

| [<IP>|<HOST-ALIAS-NAME>] | Configures the primary NetBIOS name server, using one of the following options: |
|-------------------------|--------------------------------------------------------------------------------|
|                        | • <IP> – Specifies the primary NetBIOS name server’s IP address |
|                        | • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server’s IP address |

| {<IP1>|<HOST-ALIAS-NAME1>} | Optional. Configures the secondary NetBIOS name server, using one of the following options: |
|---------------------------|-------------------------------------------------------------------------------------|
|                          | • <IP1> – Specifies the secondary NetBIOS name server’s IP address |
|                          | • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary NetBIOS name server’s IP address. If the primary NetBIOS name server is unavailable, the secondary server is used. |

**Note:** A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’ In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see `alias`.

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-name-server 192.168.13.25
```

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
    network 192.168.13.0/24
dns-server 192.168.13.9
dns-domainname mydomain.com
dns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

**Related Commands**

| `no` | Removes the NetBIOS name server settings |
12.1.3.2.13 netbios-node-type

12.1.3.2.13 netbios-node-type

 dhcp-pool-mode commands

Defines the predefined NetBIOS node type. The NetBIOS node type resolves NetBIOS names to IP addresses.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
netbios-node-type [b-node|h-node|m-node|p-node]

Parameters
- netbios-node-type [b-node|h-node|m-node|p-node]

Examples
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-node-type b-node
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
dns domainname WID
dns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
netbios-node-type b-node
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

Related Commands
no
Removes the NetBIOS node type settings
12.1.3.2.14 network

- **dhcp-pool-mode commands**

  Configures the DHCP server’s network settings

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
network [<IP/M>|<NETWORK-ALIAS-NAME>]
```

**Parameters**

- `network [<IP/M>|<NETWORK-ALIAS-NAME>]`

<table>
<thead>
<tr>
<th><strong>&lt;IP/M&gt;</strong></th>
<th>Configures the network number and mask (for example, 192.168.13.0/24)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;NETWORK-ALIAS-NAME&gt;</strong></td>
<td>Configures a network alias to identify the network number and mask</td>
</tr>
<tr>
<td><code>- &lt;NETWORK-ALIAS-NAME&gt;</code></td>
<td>Specify the network alias name. It should be existing and configured.</td>
</tr>
<tr>
<td><strong>Note:</strong> A network alias defines a single network address. For example, ‘alias network $NET 1.1.1.0/24’. In this example, the network alias name is: $NET and the network it is mapped to is: 1.1.1.0/24. For more information see, alias.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#network 192.168.13.0/24
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
dns server 192.168.13.9
dns domain-name WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

**Related Commands**

- `no` Removes the network number and mask configured for this DHCP pool
12.1.3.2.15 next-server

 dhcp-pool-mode commands

Configures the next server in the boot process

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

next-server [ <IP> | <HOST-ALIAS-NAME> ]

Parameters

- next-server [ <IP> | <HOST-ALIAS-NAME> ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>Configures the next server’s (the first server in the boot process) IP address</td>
</tr>
<tr>
<td>&lt;HOST-ALIAS-NAME&gt;</td>
<td>Configures a host alias, mapped to the next server’s IP address</td>
</tr>
<tr>
<td></td>
<td>- &lt;HOST-ALIAS-NAME&gt; – Specify the host alias name. It should be existing and configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see alias.</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#next-server 192.168.13.26

dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.23 192.168.13.29
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

Related Commands

no | Removes the next server configuration settings
12.1.3.2.16 no

* dhcp-pool-mode commands

Removes or resets this DHCP user pool’s settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [address|bootfile|ddns|default-router|dns-server|domain-name|excluded-address|
    lease|netbios-name-server|netbios-node-type|network|next-server|option|
    respond-via-unicast|static-binding|static-route|update]

no [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|
    netbios-node-type|next-server|network|respond-via-unicast]

no address [<IP>|<HOST-ALIAS-NAME>|all]
no address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]

no ddns [domainname|multiple-user-class|server|ttl]

no excluded-address [<IP>|<HOST-ALIAS-NAME>]
no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]

no option <OPTION-NAME>

no static-binding client-identifier <CLIENT-IDENTIFIER>
no static-binding hardware-address <MAC>

no static-route <IP/MASK> <GATEWAY-IP>

no update dns {override}

Parameters

- no <PARAMETERS>

no <PARAMETERS> Removes or resets this DHCP user pool’s settings

Examples

The following example shows the DHCP pool settings before the ‘no’ commands are executed:

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
network 192.168.13.0/24
    address 192.168.13.4 class dhcpclass1
    lease 100 23 59 59
ddns server 192.168.13.9
    domainname WID
ddns multiple-user-class
    excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
    netbios-node-type b-node
    bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
    netbios-name-server 192.168.13.25
    next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
The following example shows the DHCP pool settings after the 'no' commands are executed:

```
   rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
   address 192.168.13.4 class dhcpclass1
   ddns server 192.168.13.9
   ddns multiple-user-class
   excluded-address range 192.168.13.25 192.168.13.28
   netbios-node-type b-node
   dns-server 192.168.13.19
   netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```
12.1.3.2.17 option

- `dhcp-pool-mode commands`

Configures raw DHCP options. The DHCP option must be configured under the DHCP server policy. The options configured under the DHCP pool/DHCP server policy can also be used in static-bindings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
option <OPTION-NAME> [DHCP-OPTION-IP|DHCP-OPTION-ASCII]
```

Parameters

- `option <OPTION-NAME> [DHCP-OPTION-IP|DHCP-OPTION-ASCII]`

<table>
<thead>
<tr>
<th>&lt;OPTION-NAME&gt;</th>
<th>Sets the name of the DHCP option</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DHCP-OPTION-IP&gt;</td>
<td>Sets DHCP option as an IP address</td>
</tr>
<tr>
<td>&lt;DHCP-OPTION-ASCII&gt;</td>
<td>Sets DHCP option as an ASCII string</td>
</tr>
</tbody>
</table>

**NOTE:** An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show running config` to view the output). Use a double backslash to represent a single backslash.

Examples

```
> rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#option option1 157.235.208.80
> rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
> rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

- `no` Resets values or disables the DHCP pool option settings
12.1.3.2.18 **static-route**

> dhcp-pool-mode commands

Configures a static route for a DHCP pool. Static routes define a gateway for traffic intended for other networks. This gateway is always used when an IP address does not match any route in the network.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
static-route <IP/M> <IP>
```

**Parameters**

- **static-route <IP/M> <IP>**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/M&gt;</td>
<td>Specifies the IP destination prefix (for example, 10.0.0.0/8)</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Specifies the gateway IP address</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-route 192.168.13.0/24 192.168.13.7
```

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

**Related Commands**

- **no** Removes static route settings
12.1.3.2.19 respond-via-unicast

* dhcp-pool-mode commands

Sends DHCP offer and acknowledgement as unicast messages

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

respond-via-unicast

Parameters

None

Examples

rfs4000-229D58 (config-dhcp-policy-test-pool-testPool)#respond-via-unicast

rfs4000-229D58 (config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
netbios-node-type b-node
dns-server 192.168.13.19
netbios-name-server 192.168.13.25
option option1 157.235.208.80
respond-via-unicast

rfs4000-229D58 (config-dhcp-policy-test-pool-testPool)#

Related Commands

| no | Disables sending of a DHCP offer and DHCP Ack as unicast messages. When disabled, sends offer and acknowledgement as broadcast messages. |
12.1.3.2.20 update

*dhcp-pool-mode commands*

Controls the use of the DDNS service

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
update dns {override}
```

**Parameters**

- `update dns {override}`

**Usage Guidelines**

A DHCP client cannot perform updates for RR’s A, TXT and PTR resource records. Use `update (dns) (override)` to enable the internal DHCP server to send DDNS updates for resource records. The DHCP server can override the client, even if the client is configured to perform the updates.

In the DHCP server’s DHCP pool, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the DHCP server and the DNS server.

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#update dns override
```

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
    address 192.168.13.4 class dhcpclass1
    update dns override
    ddns server 192.168.13.9
    ddns multiple-user-class
    excluded-address range 192.168.13.25 192.168.13.28
    netbios-node-type b-node
    dns-server 192.168.13.19
    netbios-name-server 192.168.13.25
    option option1 157.235.208.80
    respond-via-unicast
    static-route 192.168.13.0/24 192.168.13.7
```

**Related Commands**

- `no` Removes dynamic DNS service control
12.1.3.3 static-binding

- **dhcp-pool-mode commands**

Configures static IP address information for a particular device. Static address binding is executed on the device’s hostname, client identifier, or MAC address. Static bindings allow the configuration of client parameters, such as DHCP server, DNS server, default routers, fixed IP address etc.

The following table summarizes static binding configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>static-binding</td>
<td>Creates a static binding policy and enters its config mode</td>
<td>page 12-38</td>
</tr>
<tr>
<td>static-binding-mode commands</td>
<td>Invokes static binding configuration commands</td>
<td>page 12-40</td>
</tr>
</tbody>
</table>
12.1.3.3.21 static-binding

*static-binding*

**Configures static address bindings**

A static address binding is a collection of configuration parameters, including an IP address, associated with, or bound to, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings assign IP addresses without creating numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

**Syntax**

`static-binding [client-identifier <CLIENT>|hardware-address <MAC>]`

**Parameters**

- `static-binding [client-identifier <CLIENT>|hardware-address <MAC>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identifier &lt;CLIENT&gt;</td>
<td>Enables a static binding configuration for a client based on its client identifier (as provided by DHCP option 61 and its key value)</td>
</tr>
<tr>
<td>hardware-address &lt;MAC&gt;</td>
<td>Enables a static binding configuration for a client based on its MAC address</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-binding client-identifier test

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  update dns override
d dns server 192.168.13.9
d dns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
netbios-node-type b-node
d dns-server 192.168.13.19
netbios-name-server 192.168.13.25
option option1 157.235.208.80
respond-via-unicast
static-route 192.168.13.0/24 192.168.13.7
static-binding client-identifier test
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```
DHCP static binding Mode commands:

- **bootfile** Boot file name
- **client-name** Client name
- **default-router** Default routers
- **dns-server** DNS Servers
- **domain-name** Configure domain-name
- **ip-address** Fixed IP address for host
- **netbios-name-server** NetBIOS (WINS) name servers
- **netbios-node-type** NetBIOS node type
- **next-server** Next server in boot process
- **no** Negate a command or set its defaults
- **option** Raw DHCP options
- **respond-via-unicast** Send DHCP offer and DHCP Ack as unicast messages
- **static-route** Add static routes to be installed on dhcp clients
- **clrscr** Clears the display screen
- **commit** Commit all changes made in this session
- **do** Run commands from Exec mode
- **end** End current mode and change to EXEC mode
- **exit** End current mode and down to previous mode
- **help** Description of the interactive help system
- **revert** Revert changes
- **service** Service Commands
- **show** Show running system information
- **write** Write running configuration to memory or terminal

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Resets values or disables the DHCP policy static binding settings</td>
</tr>
<tr>
<td><strong>static-binding-mode commands</strong></td>
<td>Invokes static binding configuration commands</td>
</tr>
</tbody>
</table>
12.1.3.3.22 static-binding-mode commands

The following table summarizes static binding configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootfile</td>
<td>Assigns a Bootfile name for the DHCP configuration on the network pool</td>
<td>page 12-41</td>
</tr>
<tr>
<td>client-name</td>
<td>Configures a client name</td>
<td>page 12-42</td>
</tr>
<tr>
<td>default-router</td>
<td>Configures default router or gateway IP address</td>
<td>page 12-43</td>
</tr>
<tr>
<td>dns-server</td>
<td>Sets the DNS server’s IP address available to all DHCP clients connected to the DHCP pool</td>
<td>page 12-44</td>
</tr>
<tr>
<td>domain-name</td>
<td>Sets the network pool's domain name</td>
<td>page 12-45</td>
</tr>
<tr>
<td>ip-address</td>
<td>Configures a host’s fixed IP address</td>
<td>page 12-46</td>
</tr>
<tr>
<td>netbios-name-server</td>
<td>Configures a NetBIOS (WINS) name server IP address</td>
<td>page 12-47</td>
</tr>
<tr>
<td>netbios-node-type</td>
<td>Defines the NetBIOS node type</td>
<td>page 12-48</td>
</tr>
<tr>
<td>next-server</td>
<td>Specifies the next server used in the boot process</td>
<td>page 12-49</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 12-50</td>
</tr>
<tr>
<td>option</td>
<td>Configures raw DHCP options</td>
<td>page 12-51</td>
</tr>
<tr>
<td>respond-via-unicast</td>
<td>Sends a DHCP offer and DHCP Ack as unicast messages</td>
<td>page 12-52</td>
</tr>
<tr>
<td>static-route</td>
<td>Adds static routes installed on DHCP clients</td>
<td>page 12-53</td>
</tr>
</tbody>
</table>
12.1.3.23 bootfile

static-binding-mode commands

The Bootfile command provides a diskless node the path to the image file used while booting up. Only one file can be configured for each static IP binding.

For more information on the BOOTP protocol with reference to static binding, see bootp.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
bootfile <IMAGE-FILE-PATH>
```

Parameters

- `bootfile <IMAGE-FILE-PATH>`

| <IMAGE-FILE-PATH> | Sets the path to the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted. |

Examples

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#bootfile test.txt

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
  bootfile test.txt

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

- `no` | Resets values or disables DHCP pool static binding settings
- `bootp` | Configures BOOTP protocol protocol parameters
12.1.3.3.24 client-name

*static-binding-mode commands*

Configures the client's name

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
client-name <NAME>
```

**Parameters**

- `client-name <NAME>`

**Examples**

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#client-name RFID
```

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  client-binding client-identifier test
  client-name RFID
  bootfile test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th><strong>no</strong></th>
<th>Resets values or disables DHCP pool static binding settings</th>
</tr>
</thead>
</table>

Specify the name of the client using this static IP address host pool. Do not include the domain name.
12.1.3.25 default-router

static-binding-mode commands

Configures a default router or gateway IP address for the static binding configuration

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}

Parameters

- default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}

| [<IP>|<HOST-ALIAS-NAME>] | Configures the primary default router, using one of the following options:
|--------------------------|--------------------------------------------------|
|                          | • <IP> – Specifies the primary default router’s IP address
|                          | • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router’s IP address

| {<IP1>|<HOST-ALIAS-NAME1>} | Optional. Configures the secondary default router, using one of the following options:
|---------------------------|--------------------------------------------------|
|                           | • <IP1> – Specifies the secondary default router’s IP address
|                           | • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary default router’s IP address. If the primary default router is unavailable, the secondary router is used.

Note: A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see alias.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Examples

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#default-router 172.16.10.8 172.16.10.9

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
  bootfile test.txt
  default-router 172.16.10.8 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

Related Commands

| no | Resets values or disables DHCP pool static binding settings |
### 12.1.3.3.26 dns-server

*static-binding-mode commands*

Configures the DNS server for this static binding configuration. This DNS server supports the client for which the static binding has been configured.

For this client, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dns-server [IP] | HOST-ALIAS-NAME] [IP1] | HOST-ALIAS-NAME1]

**Parameters**

- dns-server [IP] | HOST-ALIAS-NAME] [IP1] | HOST-ALIAS-NAME1]

| [IP] | HOST-ALIAS-NAME] | Configures the primary DNS server, using one of the following options:
| - IP | Specifies the primary DNS server's IP address
| - HOST-ALIAS-NAME] | Specifies a host alias, mapped to the primary DNS server's IP address

| [IP1] | HOST-ALIAS-NAME1] | Optional. Configures the secondary DNS server, using one of the following options:
| - [IP1] | Specifies the secondary DNS server's IP address
| - [HOST-ALIAS-NAME1] | Specifies a host alias, mapped to the secondary DNS server's IP address. If the primary DNS server is unavailable, the secondary DNS server is used.

**Note:** A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see *alias*.

**Examples**

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
  client-name RFID
  bootfile test.txt
  default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

**Related Commands**

| no | Resets values or disables DHCP pool static binding settings |
12.1.3.27 domain-name

Sets the domain name for the static binding configuration

Domain names are not case sensitive and contain alphabetic or numeric letters (or a hyphen). A fully qualified domain name (FQDN) consists of a host name plus a domain name. For example, computername.domain.com

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

domain-name <DOMAIN-NAME>

Parameters

- domain-name <DOMAIN-NAME>

<table>
<thead>
<tr>
<th>&lt;DOMAIN-NAME&gt;</th>
<th>Defines the domain name for the static binding configuration</th>
</tr>
</thead>
</table>

Examples

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#domain-name documentation

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
   static-binding client-identifier test
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

Related Commands

| no | Resets values or disables the DHCP pool static binding settings |
12.1.3.3.28 ip-address

- **static-binding-mode commands**

Configures a fixed IP address for a host

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

**Parameters**
- `<IP>` Configures a fixed IP address (in dotted decimal format) of the client using this host pool
- `<HOST-ALIAS-NAME>` Configures a host alias identifying the fixed IP address of the client using this host pool

**Note:** A network host alias maps a name to a single network host. For example, `alias host $HOST 1.1.1.100`. In this example the host alias is `$HOST` and it maps to a single host `1.1.1.100`. For more information, see `alias`.

**Examples**

```plaintext
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#ip-address 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context static-binding client-identifier test
  ip-address 172.16.10.9
  client-name RFID
  domain-name documentation
  bootfile test.txt
  default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets values or disable DHCP pool static binding settings</td>
</tr>
</tbody>
</table>
12.1.3.29 netbios-name-server

Configs the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

| [IP] | [HOST-ALIAS-NAME] | Configures the primary NetBIOS server, using one of the following options:
|      |                  | • <IP> – Specifies the primary NetBIOS name server’s IP address
|      |                  | • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server’s IP address
| {IP1} | [HOST-ALIAS-NAME1] | Optional. Configures the secondary NetBIOS name server, using one of the following options:
|      |                  | • <IP1> – Specifies the secondary NetBIOS name server’s IP address
|      |                  | • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary NetBIOS name server’s IP address. If the primary NetBIOS name server is unavailable, the secondary server is used.

**Note:** A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is `$HOST` and it maps to a single host ‘1.1.1.100’. For more information, see alias.

Examples

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-name-server 172.16.10.23
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
domain-name documentation
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
netbios-name-server 172.16.10.23
```

Related Commands

| no | Resets values or disables DHCP pool static binding settings |
### 12.1.3.3.30 netbios-node-type

#### static-binding-mode commands

Configures different predefined NetBIOS node types. The NetBIOS node defines the way a device resolves NetBIOS names to IP addresses.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

#### Parameters

- `netbios-node-type [b-node|h-node|m-node|p-node]`

| [b-node|h-node]| Defines the netbios node type          |
|---------------|---------------------------------------|
| m-node| p-node|---------|---------|
| b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. |
| h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. |
| m-node – Sets the node type as mixed. A mixed node uses broadcast queries to find a node, and failing that, queries a known p-node name server for the address. |
| p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine. |

#### Examples

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-node-type b-node
```

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
  client-name RFID
domain-name documentation
netbios-node-type b-node
bootfile test.txt
default-router 172.16.10.9
  172.16.10.8
  172.16.10.7
dns-server 172.16.10.7
  netbios-name-server 172.16.10.23
```

#### Related Commands

<table>
<thead>
<tr>
<th><code>no</code></th>
<th>Resets values or disables DHCP pool static binding settings</th>
</tr>
</thead>
</table>
12.1.3.31 next-server

* static-binding-mode commands

Configures the next server utilized in the boot process

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
next-server [<IP>|<HOST-ALIAS-NAME>]

Parameters
- next-server [<IP>|<HOST-ALIAS-NAME>]

<table>
<thead>
<tr>
<th>&lt;IP&gt;</th>
<th>Configures the next server’s (the first server in the boot process) IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;HOST-ALIAS-NAME&gt;</td>
<td>Configures a host alias, mapped to the next server’s IP address</td>
</tr>
</tbody>
</table>

- <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured.

**Note:** A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is ‘$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see alias.

Examples
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#next-server 172.16.10.24

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context static-binding client-identifier test
  ip-address 172.16.10.9
client-name RFID
domain-name documentation
netbios-node-type b-node
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
netbios-name-server 172.16.10.23
next-server 172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

Related Commands

no Resets values or disables DHCP pool static binding settings
12.1.3.32 no

static-binding-mode commands

Negates or reverts static binding settings for the selected DHCP server policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`no [bootfile|client-name|default-router|dns-server|domain-name|ip-address|netbios-name-server|netbios-node-type|next-server|option|respond-via-unicast|static-route]`

`no option <OPTION-NAME>`

`no static-route <IP/MASK> <GATEWAY-IP>`

Parameters

- `no <PARAMETERS>`

Examples

The following example shows the DHCP pool static binding settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
  ip-address 172.16.10.9
  client-name RFID
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
  netbios-name-server 172.16.10.23
  next-server 172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no bootfile
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no ip-address
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no default-router
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no dns-server
```

The following example shows the DHCP pool static binding settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
  client-name RFID
  domain-name documentation
  netbios-node-type b-node
  netbios-name-server 172.16.10.23
  next-server 172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```
12.1.3.33 option

static-binding-mode commands

Configures the raw DHCP options in the DHCP policy. The DHCP options can be used only in static bindings.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```bash
option <OPTION-NAME> [ <DHCP-OPTION-IP> | <DHCP-OPTION-ASCII> ]
```

Parameters

- `<OPTION-NAME>`
  - Sets the DHCP option name
- `<DHCP-OPTION-IP>`
  - Sets the DHCP option as an IP address
- `<DHCP-OPTION-ASCII>`
  - Sets the DHCP option as an ASCII string

Usage Guidelines

Defines non standard DHCP option codes (0-254)

**NOTE:** An option name in ASCII format accepts a backslash (`\`) as an input, but is not displayed in the output (Use `show running config` to view the output). Use a double backslash to represent a single backslash.

Examples

```bash
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#option option1 172.16.10.10

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context static-binding client-identifier test client-name RFID domain-name documentation netbios-node-type b-node netbios-name-server 172.16.10.23 next-server 172.16.10.24

option option1 172.16.10.10

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```
**12.1.3.3.34 respond-via-unicast**

- **Static-binding-mode commands**

  Sends a DHCP offer and DHCP acknowledge as unicast messages

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
respond-via-unicast
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#respond-via-unicast
```

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
  client-name RFID
  domain-name documentation
  netbios-node-type b-node
  netbios-name-server 172.16.10.23
  next-server 172.16.10.24
  option option1 172.16.10.10
  respond-via-unicast
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Resets values or disables DHCP pool static binding settings</td>
</tr>
</tbody>
</table>
12.1.3.35 static-route

- static-binding-mode commands

Adds static routes to the static binding configuration

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
static-route <IP/MASK> <GATEWAY-IP>

Parameters
- static-route <IP/MASK> <GATEWAY-IP>

<table>
<thead>
<tr>
<th>&lt;IP/MASK&gt;</th>
<th>Sets the subnet for which the static route is configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;GATEWAY-IP&gt;</td>
<td>Specify the gateway’s IP address</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#static-route 10.0.0.0/10 157.235.208.235

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
domain-name documentation
netbios-node-type b-node
netbios-name-server 172.16.10.23
next-server 172.16.10.24
option option1 172.16.10.10
respond-via-unicast
static-route 10.0.0.0/10 157.235.208.235
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

Related Commands
- no
  Resets values or disables DHCP pool static route settings
**12.1.4 dhcp-server**

- **dhcp-server-policy**

  Configures the activation-criteria (run-criteria) that triggers dynamic activation of DHCP service running on a redundancy device.

  In a managed wireless network, when the primary, active DHCP server fails (is unreachable), network clients are unable to access DHCP services, such as new IP address leasing and renewal of existing IP address leases. In such a scenario, the activation-criteria, when configured, triggers dynamic activation of the secondary DHCP server, allowing network clients to continue accessing DHCP services. The WiNG implementation provides activation-criteria options specific to a RF Domain, cluster setup, and a *Virtual Router Redundancy Protocol (VRRP)* master/client setup.

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master]
```

**Parameters**

- **dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master]**

<table>
<thead>
<tr>
<th>dhcp-server</th>
<th>Enables dynamic activation of the DHCP server, running on a redundancy device, based on the activation criteria specified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>activation-criteria [cluster-master</td>
<td>rf-domain-manager</td>
</tr>
<tr>
<td></td>
<td>• cluster-master – Configures the cluster-master criteria in a cluster setup. Within a cluster, DHCP service is enabled on the cluster master. While it remains disabled on the other cluster members. In case of the cluster master failing, the cluster-master activation criteria, when configured, triggers dynamic activation of DHCP service on the new cluster master.</td>
</tr>
<tr>
<td></td>
<td>• rf-domain-manager – Configures the rf-domain-manager criteria on an RF Domain. Within a RF Domain, DHCP service is enabled on the RF Domain manager. While it remains disabled on the other devices within the RF Domain. In case of the RF Domain manager failing, the rf-domain-manager activation criteria, when configured, triggers dynamic activation of DHCP service on the new RF Domain manager.</td>
</tr>
<tr>
<td></td>
<td>• vrrp-master – Configures the vrrp-master criteria within a VRRP master/client setup. In such a setup, the DHCP service is enabled on the VRRP master. While it remains disabled on the other members. In case of the VRRP master failing, the vrrp-master activation criteria, when configured, triggers dynamic activation of DHCP service on the new VRRP master.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test)#dhcp-server activation-criteria rf-domain-manager

rfs4000-229D58(config-dhcp-policy-test)#show context
dhcp-server-policy test
dhcp-server activation-criteria rf-domain-manager

rfs4000-229D58(config-dhcp-policy-test)#

rfs4000-229D58(config-dhcp-policy-test)#no dhcp-server activation-criteria
```
rfs4000-229D58(config-dhcp-policy-test)#show context
dhcp-server-policy test
rfs4000-229D58(config-dhcp-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the DHCP service activation criteria configured on this DHCP server policy</td>
</tr>
</tbody>
</table>
12.1.5 no

`dhcp-server-policy`

Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [bootp|dhcp-class|dhcp-pool|dhcp-server|option|ping]

no bootp ignore
no dhcp-class <DHCP-CLASS-NAME>
no dhcp-pool <DHCP-POOL-NAME>
no dhcp-server activation-criteria
no option <DHCP-OPTION>
no ping timeout
```

**Parameters**

- `no <PARAMETERS>`,Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings.

**Examples**

The following example shows the DHCP policy 'test' settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
  bootp ignore
dhcp-class dhcpclass1
dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  update dns override
  --More--
rfs7000-37FABE(config-dhcp-policy-test)#
```

```
rfs7000-37FABE(config-dhcp-policy-test)#no bootp ignore
rfs7000-37FABE(config-dhcp-policy-test)#no dhcp-class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test)#no dhcp-pool pool1
```

The following example shows the DHCP policy 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
rfs7000-37FABE(config-dhcp-policy-test)#
```
12.1.6 Option

Option

Syntax

Parameters

Usage Guidelines

Defined non-standard DHCP option codes (0-254)

Examples

Related Commands

NOTE: An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (Use show running config to view the output). Use a double backslash to represent a single backslash.

Configures raw DHCP options. The DHCP option has to be configured in the DHCP server policy. The options configured in the DHCP pool/DHCP server policy can also be used in static bindings.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Option <OPTION-NAME> <0-254> [ascii|hexstring|ip]

- OPTION-NAME: Configures the option name
- 0-254: Configures the DHCP option code from 0 - 254
- ascii: Configures the DHCP option as an ASCII string
- hexstring: Configures the DHCP option as a hexadecimal string
- ip: Configures the DHCP option as an IP address

Define non-standard DHCP option codes (0-254)
12.1.7 ping

dhcp-server-policy

Configures the DHCP server’s ping timeout interval. The controller uses the timeout to intermittently ping and discover whether a client requested IP address is available or in use.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ping timeout <1-10>`

**Parameters**

- `ping timeout <1-10>`

  **timeout <1-10>**

  Sets the ping timeout from 1 - 10 seconds. The default is 1 second.

**Examples**

```
rfs7000-37FABE(config-dhcp-policy-test)#ping timeout 2
rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
  ping timeout 2
  option option1 200 ascii
rfs7000-37FABE(config-dhcp-policy-test)#
```

**Related Commands**

```
no
```

Resets the ping interval to 1 second
12.2 dhcpv6-server-policy

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

The following table summarizes DHCPv6 server policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcpv6-pool</td>
<td>Creates a DHCPv6 pool and enters its configuration mode</td>
<td>page 12-60</td>
</tr>
<tr>
<td>option</td>
<td>Configures this DHCPv6 server policy’s DHCP option settings, such as enterprise (vendor ID)</td>
<td>page 12-71</td>
</tr>
<tr>
<td>restrict-vendor-options</td>
<td>Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy</td>
<td>page 12-73</td>
</tr>
<tr>
<td>server-preference</td>
<td>Configures this DHCP server’s preference value. This value is sent in DHCP server replies to the IPv6 client.</td>
<td>page 12-74</td>
</tr>
<tr>
<td>no</td>
<td>Negates or reverts this DHCPv6 server policy’s settings</td>
<td>page 12-75</td>
</tr>
</tbody>
</table>
12.2.1 dhcpv6-pool

The following table summarizes DHCPv6 pool configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcpv6-pool</td>
<td>Creates a DHCPv6 pool and enters its configuration mode</td>
<td>page 12-61</td>
</tr>
<tr>
<td>dhcpv6-pool-mode</td>
<td>Summarizes DHCPv6 pool configuration mode commands</td>
<td>page 12-63</td>
</tr>
</tbody>
</table>
12.2.1.1 dhcpv6-pool

```
 dhcv6-pool
```

Configures a DHCPv6 server address pool and enters its configuration mode

A DHCPv6 IPv6 pool is a resource from which IPv6 formatted addresses can be issued on DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
dhcpv6-pool <POOL-NAME>
```

Parameters

- `dhcpv6-pool <POOL-NAME>`

Examples

```
rfs7000-37FABE(config-dhcpv6-server-policy-test)#dhcpv6-pool DHCPv6Pool1
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#?
DHCPv6 pool Mode commands:
dns-server DNS Servers
domain-name Configure domain-name
network Network on which DHCPv6 server will be deployed
no Negate a command or set its defaults
option Raw DHCPv6 options
refresh-time Upper limit specifying the timer for which client should wait before refreshing information
sip SIP server options
c clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
rfs7000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
dhcpv6-pool DHCPv6Pool1
  network 2002::/64
domain-name TechPubs
  sip domain-name TechPubsSIP
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the DHCPv6 pool identified by the <code>&lt;POOL-NAME&gt;</code> keyword</td>
</tr>
</tbody>
</table>
12.2.1.2  dhcpv6-pool-mode commands

- **dhcpv6-pool**

Configures the DHCPv6 pool parameters

The following table summarizes DHCPv6 pool configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-server</td>
<td>Configures this DHCPv6 pool’s DNS server</td>
<td>page 12-64</td>
</tr>
<tr>
<td>domain-name</td>
<td>Configures this DHCPv6 pool’s domain name</td>
<td>page 12-65</td>
</tr>
<tr>
<td>network</td>
<td>Configures this DHCPv6 pool’s network</td>
<td>page 12-66</td>
</tr>
<tr>
<td>option</td>
<td>Configures this DHCPv6 pool’s raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool.</td>
<td>page 12-68</td>
</tr>
<tr>
<td>refresh-time</td>
<td>Configures this DHCPv6 pool’s refresh time in seconds</td>
<td>page 12-69</td>
</tr>
<tr>
<td>sip</td>
<td>Configures this DHCPv6 pool’s Session Initiation Protocol (SIP) server setting</td>
<td>page 12-70</td>
</tr>
<tr>
<td>no</td>
<td>Negates or reverts this DHCPv6 pool’s settings</td>
<td>page 12-67</td>
</tr>
</tbody>
</table>
## 12.2.1.2.36 dns-server

**dhcpv6-pool-mode commands**

Configures this DHCPv6 pool’s DNS server. The DNS server supports all clients connected to networks supported by the DHCPv6 server.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dns-server <IPv6> {<SECONDARY-IPv6>}

**Parameters**

- **dns-server <IPv6> {<SECONDARY-IPv6>}**

<table>
<thead>
<tr>
<th>&lt;IPv6&gt;</th>
<th>Configures the primary DNS server’s IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* &lt;IPv6&gt; – Specify the DNS server’s IPv6 address (the server associated with this DHCP pool).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;SECONDARY-IPv6&gt;</th>
<th>Configures the secondary DNS server’s IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* &lt;SECONDARY-IPv6&gt; – Specify the secondary DNS server’s IPv6 address (the server associated with this DHCP pool).</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context dhcpv6-pool DHCPv6Pool1
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

**Related Commands**

- **no** | Removes this DHCPv6 pool’s configured DNS server settings
12.2.1.2.37 domain-name

- dhcpv6-pool-mode commands

Configures this DHCPv6 pool's domain name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

domain-name <DOMAIN-NAME>

Parameters
- domain-name <DOMAIN-NAME>

| <DOMAIN-NAME> | Specify the DHCP pool's hostname or hostnames of the domain or domains |

Examples

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#domain-name TechPubs

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
domain-name TechPubs
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#

Related Commands

- no Removes this DHCPv6 pool's domain name
### 12.2.1.2.38 network

* dhcpv6-pool-mode commands

Configures this DHCPv6 pool's network. Use this command to configure the address of the network on which this DHCP server is deployed.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
network [IPv6/M] [NETWORK-ALIAS-NAME]
```

**Parameters**
- `network [IPv6/M] [NETWORK-ALIAS-NAME]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv6/M&gt;</code></td>
<td>Specify this DHCPv6 pool network's IPv6 address and mask (for example, 1:2::1:0/96)</td>
</tr>
<tr>
<td><code>&lt;NETWORK-ALIAS-NAME&gt;</code></td>
<td>Specify this DHCPv6 pool network's alias name</td>
</tr>
</tbody>
</table>

**Examples**
```
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#network 2002::0/64
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
  network 2002::/64
domain-name TechPubs
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

**Related Commands**
```
no
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the network IPv6 address and mask configured for this DHCPv6 pool</td>
</tr>
</tbody>
</table>
12.2.1.2.39 no

^ dhcpv6-pool-mode commands

Negates a command or sets its default. When used in the DHCPv6 pool configuration context, the ‘no’ command resets or reverts the DHCPv6 pool’s settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
no [dns-server|domain-name|network|option|refresh-time|sip]

Parameters
- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Negates a command or sets its default. When used in the DHCPv6 pool configuration context, the ‘no’ command resets or reverts the DHCPv6 pool's settings.</th>
</tr>
</thead>
</table>

Examples

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    refresh-time 1000
    domain-name TechPubs
    sip domain-name TechPubsSIP
dns-server 2002::1
    option DHCPv6Pool1Option 60
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#no option
DHCPv6Pool1Option

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#no refresh-time

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    domain-name TechPubs
    sip domain-name TechPubsSIP
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
12.2.1.2.40 option

**dhcpv6-pool-mode commands**

Configures this DHCPv6 pool's raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
option <OPTION-NAME> [ <DHCPv6-OPTION-IP> | <DHCPv6-OPTION-ASCII> ]
```

**Parameters**

- `option <OPTION-NAME> [ <DHCPv6-OPTION-IP> | <DHCPv6-OPTION-ASCII> ]`

<table>
<thead>
<tr>
<th>&lt;OPTION-NAME&gt;</th>
<th>Sets the name of the DHCPv6 option</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DHCPv6-OPTION-IP&gt;</td>
<td>Sets DHCPv6 option as an IPv6 address</td>
</tr>
<tr>
<td>&lt;DHCPv6-OPTION-ASCII&gt;</td>
<td>Sets DHCPv6 option as an ASCII string</td>
</tr>
</tbody>
</table>

**NOTE:** An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use show running config to view the output). Use a double backslash to represent a single backslash.

**Examples**

```
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#option DHCPv6Pool1Option 60
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    domain-name TechPubs
dns-server 2002::1
option DHCPv6Pool1Option 60
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

**Related Commands**

```
no
```

Removes this DHCPv6 pool's DHCP option settings
### 12.2.1.2.41 refresh-time

`dhcpv6-pool-mode commands`

Configures this DHCPv6 pool’s refresh time in seconds. This is the interval between two successive DHCP pool refreshes. The DHCP refresh process refreshes IPv6 client information.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
refresh-time <600-4294967295>
```

**Parameters**

- `refresh-time <600-4294967295>`

**Examples**

```plaintext
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#refresh-time 1000
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  refresh-time 1000
  domain-name TechPubs
dns-server 2002::1
  option DHCPv6Pool1Option 60
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes or reverts the configured DHCPv6 pool’s refresh time</td>
</tr>
</tbody>
</table>
12.2.1.2.42 sip

`dhcpv6-pool-mode commands`

Configures this DHCPv6 pool’s Session Initiation Protocol (SIP) server setting.

Configures the domain name or domain names associated with the SIP servers. The SIP server is used to prioritize voice and video traffic on the network. SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several components (user agents, proxy servers, redirect servers, and registrars). User agents can contain SIP clients; proxy servers always contain SIP clients.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
sip [address <IPv6>|domain-name <DOMAIN-NAME>]
```

**Parameters**

- `sip [address <IPv6>|domain-name <DOMAIN-NAME>]`

**Examples**

```
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#sip domain-name TechPubs

rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  refresh-time 1000
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
  option DHCPv6Pool1Option 60
rfs7000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

**Related Commands**

- `no` | Removes this DHCPv6 pool’s SIP server setting
12.2.2 option

dhcpv6-server-policy

Configures this DHCPv6 server policy’s DHCP option settings, such enterprise (vendor) ID.

DHCPv6 services are available for specific IP interfaces. A pool (or range) of IPv6 network addresses and DHCPv6 options can be created for each IPv6 interface defined. This range of addresses can be made available to DHCPv6 enabled devices on either a permanent or leased basis. DHCPv6 options are provided to each client with a DHCPv6 response and provide DHCPv6 clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCPv6 client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCPv6 client.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
option <OPTION-NAME> <0-254> [ascii|hexstring|ipv6] <1-4294967295>
```

Parameters

- option <OPTION-NAME> <0-254> [ascii|hexstring|ipv6] <1-4294967295>

<table>
<thead>
<tr>
<th>option</th>
<th>Specify a unique name for this DHCP option. The name should describe option’s function.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-254&gt;</td>
<td>Specify a DHCP option code for this option.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-254&gt; – Specify a value from 0 -254.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system allows only one code, of the same value, for each DHCP option used</td>
</tr>
<tr>
<td></td>
<td>in each DHCPv6 server policy.</td>
</tr>
</tbody>
</table>

| ascii   | Specifies the option type as ASCII (sends an ASCII compliant string to the client)        |
| hexstring | Specifies the option type as a string of hexadecimal characters (sends a hexadecimal    |
| ipv6    | Specifies the option type as IPv6 address (sends an IPv6 compatible address to the client) |
| <1-4294967295> | This parameter is common to all option types.                                           |
|         | • <1-4294967295> – Specifies the enterprise (vendor) ID. Specify a value from 1 -     |
|         | 4294967295. The option code (1) is reserved for subnet-mask and cannot be used.         |
|         | **Note:** Each vendor should have a unique vendor ID used by the DHCP server to issue   |
|         | vendor-specific DHCP options.                                                            |
Examples
rfs7000-37FABE(config-dhcpv6-server-policy-test)#option DHCPServerOption1 10 ascii 50
rfs7000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
  option DHCPServerOption1 10 ascii 50
dhcpv6-pool DHCPv6Pool1
  network 2002::/64
domain-name TechPubs
  sip domain-name TechPubsSIP
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the DHCPv6 server option settings configured for this DHCPv6 server policy</td>
</tr>
</tbody>
</table>
12.2.3 restrict-vendor-options

Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy. When restricted, vendor-specific DHCP options, configured on this DHCPv6 server policy, are not included in the DHCPv6 server replies to IPv6 clients.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

restrict-vendor-options

Parameters

None

Examples

rfs7000-37FABE(config-dhcpv6-server-policy-test)#restrict-vendor-options

rfs7000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
  option DHCPServerOption1 10 ascii 50
dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    domain-name TechPubs
    sip domain-name TechPubsSIP
dns-server 2002::1
  restrict-vendor-options
rfs7000-37FABE(config-dhcpv6-server-policy-test)#

Related Commands

| no | Removes restriction on sending of vendor-specific options in DHCPv6 server replies to IPv6 clients |
12.2.4 server-preference

`dhcpv6-server-policy`

Configures this DHCPv6 server's preference value. When configured, the server preference value is included in the DHCPv6 server's replies to IPv6 clients.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
```
server-preference <0-255>
```

Parameters
- `server-preference <0-255>`

Examples
```
rfs7000-37FABE(config-dhcpv6-server-policy-test)#server-preference 1

rfs7000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
  option DHCPServerOption1 10 ascii 50
dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    domain-name TechPubs
    sip domain-name TechPubsSIP
dns-server 2002::1
  server-preference 1
  restrict-vendor-options
rfs7000-37FABE(config-dhcpv6-server-policy-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes this DHCPv6 server's preference value</td>
</tr>
</tbody>
</table>
12.2.5 no

Negates or reverts this DHCPv6 server policy's settings

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [dhcpv6-pool|option|restrict-vendor-options|server-preference]

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Negates or reverts this DHCPv6 server policy's settings |

Examples

rfs7000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
  option DHCPServerOption1 10 ascii 50
dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    domain-name TechPubs
    sip domain-name TechPubsSIP
dns-server 2002::1
  server-preference 1
  restrict-vendor-options
rfs7000-37FABE(config-dhcpv6-server-policy-test)#

rfs7000-37FABE(config-dhcpv6-server-policy-test)#no restrict-vendor-options
rfs7000-37FABE(config-dhcpv6-server-policy-test)#no server-preference

rfs7000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
  option DHCPServerOption1 10 ascii 50
  dhcpv6-pool DHCPv6Pool1
    network 2002::/64
    domain-name TechPubs
    sip domain-name TechPubsSIP
dns-server 2002::1
rfs7000-37FABE(config-dhcpv6-server-policy-test)#
This chapter summarizes the firewall policy commands in the CLI command structure.

A firewall protects a network from attacks and unauthorized access from outside the network. Simultaneously, it allows authorized users to access required resources. Firewalls work on multiple levels. Some work at layers 1, 2 and 3 to inspect each packet. The packet is either passed, dropped or rejected based on rules configured on the firewall.

Firewalls use application layer filtering to enforce compliance. These firewalls can understand applications and protocols and can detect if an unauthorized protocol is being used, or an authorized protocol is being abused in any malicious way.

The third set of firewalls, ‘Stateful Firewalls’, consider the placement of individual packets within each packet in the series of packets being transmitted. If there is a packet that does not fit into the sequence, it is automatically identified and dropped.

Use (config) instance to configure firewall policy commands. To navigate to the config-fw-policy instance, use the following commands:

```
<DEVICE>(config)#firewall-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#?
```

**Firewall policy Mode commands:**

- acl-logging: Log on flow creating traffic
- alg: Enable ALG
- clamp: Clamp value
- dhcp-offer-convert: Enable conversion of broadcast dhcp offers to unicast
- dns-snoop: DNS Snooping
- firewall: Wireless firewall
- flow: Firewall flow
- ip: Internet Protocol (IP)
- ip-mac: Action based on ip-mac table
- ipv6: Internet Protocol version 6 (IPv6)
- ipv6-mac: Action based on ipv6-mac table
- logging: Firewall enhanced logging
- no: Negate a command or set its defaults
- proxy-arp: Enable generation of ARP responses on behalf of another device
- proxy-nd: Enable generation of ND responses (for IPv6) on behalf of another device
- stateful-packet-inspection-l2: Enable stateful packet inspection in layer2 firewall
- storm-control: Storm-control
- virtual-defragmentation: Enable virtual defragmentation for IPv4 packets (recommended for proper functioning
of firewall)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config-fw-policy-test)#

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore `_` character. In other words, the name of a device cannot contain an underscore.
## 13.1 firewall-policy

The following table summarizes default firewall policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-logging</td>
<td>Enables logging on flow creating traffic</td>
<td>page 13-4</td>
</tr>
<tr>
<td>alg</td>
<td>Enables an algorithm</td>
<td>page 13-5</td>
</tr>
<tr>
<td>clamp</td>
<td>Sets a clamp value to limit TCP MSS to inner path-MTU for tunnelled packets</td>
<td>page 13-7</td>
</tr>
<tr>
<td>dhcp-offer-convert</td>
<td>Enables the conversion of broadcast DHCP offers to unicast</td>
<td>page 13-8</td>
</tr>
<tr>
<td>dns-snoop</td>
<td>Sets the timeout value for DNS entries</td>
<td>page 13-9</td>
</tr>
<tr>
<td>firewall</td>
<td>Configures the wireless firewall</td>
<td>page 13-10</td>
</tr>
<tr>
<td>flow</td>
<td>Defines a session flow timeout</td>
<td>page 13-11</td>
</tr>
<tr>
<td>ip</td>
<td>Configures Internet Protocol (IP) components on this firewall policy</td>
<td>page 13-13</td>
</tr>
<tr>
<td>ip-mac</td>
<td>Defines an action based on IP-MAC table</td>
<td>page 13-20</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures IPv6 components on this firewall policy</td>
<td>page 13-23</td>
</tr>
<tr>
<td>ipv6-mac</td>
<td>Defines an action based on IPv6-MAC table</td>
<td>page 13-26</td>
</tr>
<tr>
<td>logging</td>
<td>Enables enhanced firewall logging</td>
<td>page 13-28</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 13-30</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>Enables the generation of ARP responses on behalf of another device</td>
<td>page 13-32</td>
</tr>
<tr>
<td>proxy-nd</td>
<td>Enables the generation of ND responses (for IPv6) on behalf of another device</td>
<td>page 13-33</td>
</tr>
<tr>
<td>stateful-packet-inspection-12</td>
<td>Enables stateful packets-inspection in layer 2 firewall</td>
<td>page 13-34</td>
</tr>
<tr>
<td>storm-control</td>
<td>Defines storm control and logging settings</td>
<td>page 13-35</td>
</tr>
<tr>
<td>virtual-defragmentation</td>
<td>Enables virtual defragmentation of IPv4 packets</td>
<td>page 13-37</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *Chapter 5, COMMON COMMANDS.*
13.1.1 acl-logging

- **firewall-policy**

Enables logging on flow creating traffic

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
acl-logging

Parameters
None

Examples

rfs4000-229D58(config-fw-policy-test)#acl-logging

rfs4000-229D58(config-fw-policy-test)#no acl-logging

rfs4000-229D58(config-fw-policy-test)#show context firewall-policy test
  no ip dos tcp-sequence-past-window
  no acl-logging
rfs4000-229D58(config-fw-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables logging on flow creating traffic</td>
</tr>
</tbody>
</table>
### 13.1.2 alg

**firewall-policy**

Enables traffic filtering at the application layer using the Application Layer Gateway (ALG) feature.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
alg [dns|facetime|ftp|pptp|sccp|sip|tftp]
```

**Parameters**

- `alg [dns|facetime|ftp|pptp|sccp|sip|tftp]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>Allows Domain Name System (DNS) traffic through the firewall using its default ports. This option is enabled by default. When enabled, you can easily permit or deny traffic based on a packet’s DNS name, instead of the IP address. Use this option when configuring ACLs allowing or denying traffic for Web sites that have a single domain name resolving to any one of multiple IP addresses.</td>
</tr>
<tr>
<td>facetime</td>
<td>Allows Apple’s FaceTime video calling traffic through the firewall using its default ports. This option is enabled by default.</td>
</tr>
<tr>
<td>ftp</td>
<td>Allows File Transfer Protocol (FTP) traffic through the firewall using its default ports. This option is enabled by default.</td>
</tr>
<tr>
<td>pptp</td>
<td>Allows Point-to-Point Tunneling Protocol (PPTP) traffic through the firewall using its default ports. PPTP, a network protocol, enables secure transfer of data from a remote client to an enterprise server by encapsulating PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. This option is enabled by default.</td>
</tr>
<tr>
<td>sccp</td>
<td>Allows Signalling Connection Control Part (SCCP) traffic through the firewall using its default ports. This option is disabled by default. SCCP is a network protocol that provides routing, flow control and error correction in telecommunication networks.</td>
</tr>
<tr>
<td>sip</td>
<td>Allows Session Initiation Protocol (SIP) traffic through the firewall using its default ports. This option is enabled by default.</td>
</tr>
<tr>
<td>tftp</td>
<td>Enables the Trivial File Transfer Protocol (TFTP) algorithm. When enabled, allows TFTP traffic through the firewall using its default ports. This option is enabled by default.</td>
</tr>
</tbody>
</table>
Examples
nx4500-5CFA2B(config-fw-policy-test)#alg facetime
nx4500-5CFA2B(config-fw-policy-test)#show context firewall-policy test
   no ip dos tcp-sequence-past-window
   alg facetime
nx4500-5CFA2B(config-fw-policy-test)#

Related Commands

| no          | Removes or reverts ALG related settings |
13.1.3 clamp

**firewall-policy**

This option limits the TCP *Maximum Segment Size* (MSS) to the size of the *Maximum Transmission Unit* (MTU) discovered by path MTU discovery for the inner protocol. This ensures the packet traverses through the inner protocol without fragmentation. This option is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

clamp tcp-mss

**Parameters**
- clamp tcp-mss

<table>
<thead>
<tr>
<th>tcp-mss</th>
<th>Limits the TCP MSS size to the MTU value of the inner protocol for tunneled packets</th>
</tr>
</thead>
</table>

**Examples**

rfs7000-37FABE(config-fw-policy-test)#clamp tcp-mss

**Related Commands**

| no | Disables limiting of the TCP MSS |
13.1.4 dhcp-offer-convert

Enables the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-offer-convert

Parameters

None

Examples

rfs7000-37FABE(config-fw-policy-test)#dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
  no ip dos tcp-sequence-past-window
dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-test)#

Related Commands

| no | Disables the conversion of broadcast DHCP offers to unicast |
13.1.5 **dns-snoop**

Sets the timeout interval for DNS snoop table entries. DNS snoop entries provide information, such as client to IP address and client to default gateway(s) mappings. This information is used to detect if the client is sending routed packets to a wrong MAC address.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dns-snoop entry-timeout <30-86400>

**Parameters**

- dns-snoop entry-timeout <30-86400>

| entry-timeout <30-86400> | Sets the DNS snoop table entry timeout interval from 30 - 86400 seconds. An entry is retained in the DNS snoop table only for the specified time, and is deleted once this time is exceeded. The default is 1,800 seconds. |

**Examples**

rfs7000-37FABE(config-fw-policy-test)#dns-snoop entry-timeout 35

rfs7000-37FABE(config-fw-policy-test)#show context firewall-policy test
no ip dos tcp-sequence-past-window
dhcp-offer-convert
dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#

**Related Commands**

- no | Removes the DNS snoop table entry timeout interval
13.1.6 firewall

- **firewall-policy**
  Enables a device's firewall
  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
firewall enable
```

**Parameters**

- ```firewall enable``` Enables wireless firewalls

**Examples**

```plaintext
rfs7000-37FABE(config-fw-policy-default)#firewall enable
rfs7000-37FABE(config-fw-policy-default)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables a device's firewall</td>
</tr>
</tbody>
</table>
13.1.7 flow

Defined the session flow timeout interval for different packet types

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

flow [dhcp|timeout]

flow dhcp stateful

flow timeout [icmp|other|tcp|udp]

flow timeout [icmp|other] <1-32400>

flow timeout udp <15-32400>

flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|stateless-general] <1-32400>

flow timeout tcp established <15-32400>

Parameters

- flow dhcp stateful

  dhcp | Configure DHCP packet flow

  stateful | Performs a stateful check on DHCP packets. This feature is enabled by default.

- flow timeout [icmp|other] <1-32400>

  timeout | Configure a packet timeout

  icmp | Configure the timeout for ICMP packets. The default is 30 seconds.

  other | Configure the timeout for packets other than ICMP, TCP, or UDP. The default is 30 seconds.

  <1-32400> | Configure the timeout from 1 - 32400 seconds

- flow timeout udp <15-32400>

  timeout | Configure a packet timeout

  udp | Configure the timeout for UDP packets. The default is 30 seconds.

  <15-32400> | Configure the timeout from 15 - 32400 seconds

- flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|stateless-general] <1-32400>

  timeout | Configure a packet timeout

  tcp | Configure the timeout for TCP packets

  close-wait | Configure the closed TCP flow timeout. The default is 10 seconds.

  reset | Configure the reset TCP flow timeout. The default is 10 seconds.

  setup | Configure the opening TCP flow timeout. The default is 10 seconds.
### Examples

```bash
rfs7000-37FABE(config-rw-policy-test)#flow timeout udp 10000
rfs7000-37FABE(config-rw-policy-test)#flow timeout icmp 16000
rfs7000-37FABE(config-rw-policy-test)#flow timeout other 16000
rfs7000-37FABE(config-rw-policy-test)#flow timeout tcp established 1500
```

```bash
rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
  no ip dos tcp-sequence-past-window
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
dhcp-offer-convert
dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

### Related Commands

- `no`: Removes session timeout intervals configured for different packet types
13.1.8 ip

firewall-policy

Configures Internet Protocol (IP) components

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ip [dos|tcp]


ip tcp adjust-mss <472-1460>

Parameters


<table>
<thead>
<tr>
<th>dos</th>
<th>Identifies IP events as DoS events</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascend</td>
<td>Optional. Detects ASCEND DoS attacks</td>
</tr>
<tr>
<td></td>
<td>Ascend DoS attacks target known vulnerabilities in various versions of Ascend routers. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| broadcast-multicast-icmp | Optional. Detects broadcast or multicast ICMP DoS attacks
Broadcast or multicast ICMP DoS attacks take advantage of ICMP behavior in response to echo replies. These attacks spoof the source address of the target and send ICMP broadcast or multicast echo requests to the rest of the network, flooding the target machine with replies. |
| chargen            | Optional. Detects Chargen attacks
The Character Generation Protocol (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements.
The Chargen attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services. |
| fraggle            | Optional. Detects Fraggle DoS attacks
The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic. |
| ftp-bounce         | Optional. Detects FTP bounce attacks
A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client. |
| invalid-protocol   | Optional. Enables a check for an invalid protocol number
Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack. |
| ip-ttl-zero        | Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)
The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a *Time to Live* (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload. |
| ipsproof           | Optional. Enables a check for the IP spoofing DoS attacks
IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker. |
| land               | Optional. Detects LAND DoS attacks
A *Local Area Network Denial* (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously. |
<p>| option-route       | Optional. Enables an IP Option Record Route DoS check |</p>
<table>
<thead>
<tr>
<th><strong>router-advt</strong></th>
<th>Optional. Detects router-advertisement attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This attack uses ICMP to redirect the network router function to some other host. If that host cannot provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the ‘false’ router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>router-solicit</strong></th>
<th>Optional. Detects router solicitation attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The ICMP router solicitation scan is used to actively find routers on a network. A hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests.</td>
</tr>
</tbody>
</table>

| **smurf** | Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies. |

| **snork** | Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU’s resources. This attack uses a UDP packet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack. |

| **tcp-bad-sequence** | Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TCP connection |

<table>
<thead>
<tr>
<th><strong>tcp-fin-scan</strong></th>
<th>Optional. Detects TCP FIN scan attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the Finish (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. If the target device’s TCP port is closed, the target device sends a TCP RST packet in reply. If the target device’s TCP port is open, the target device discards the FIN and sends no reply.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tcp-intercept</td>
<td>Optional. Prevents TCP intercept attacks by using TCP SYN cookies. A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overpowers the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing e-mail, using FTP service, and so on. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software’s aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests. When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.</td>
</tr>
<tr>
<td>tcp-null-scan</td>
<td>Optional. Detects TCP NULL scan attacks. Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings. If the target device’s TCP port is closed, the target device sends a TCP RST packet in reply. If the target device’s TCP port is open, the target discards the TCP NULL scan, sending no reply.</td>
</tr>
<tr>
<td>tcp-post-syn</td>
<td>Optional. Detects TCP post SYN DoS attacks. A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an Intrusion Detection System (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS.</td>
</tr>
<tr>
<td>tcp-sequence-past-window</td>
<td>Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP’s TCP stack which sends data past the window when conducting a selective ACK.</td>
</tr>
<tr>
<td>tcp-xmas-scan</td>
<td>Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.</td>
</tr>
<tr>
<td>tcphdrfrag</td>
<td>Optional. A DoS attack where the TCP header spans IP fragments.</td>
</tr>
<tr>
<td>twinge</td>
<td>Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>udp-short-hdr</td>
<td>Optional. Enables the identification of truncated UDP headers and UDP header length fields</td>
</tr>
<tr>
<td>winnuke</td>
<td>Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT. The WINNUKE DoS attack sends a</td>
</tr>
<tr>
<td></td>
<td>large amount of data to UDP port 137 to crash the NETBIOS service on windows and results in high CPU</td>
</tr>
<tr>
<td></td>
<td>utilization on the target machine.</td>
</tr>
<tr>
<td>log-and-drop</td>
<td>Logs the event and drops the packet</td>
</tr>
<tr>
<td>log-only</td>
<td>Logs the event only, the packet is not dropped</td>
</tr>
<tr>
<td>log-level</td>
<td>Configures the log level</td>
</tr>
<tr>
<td>&lt;0-7&gt;</td>
<td>Sets the numeric logging level</td>
</tr>
<tr>
<td>emergencies</td>
<td>Numerical severity 0. System is unusable</td>
</tr>
<tr>
<td>alerts</td>
<td>Numerical severity 1. Indicates a condition where immediate action is required</td>
</tr>
<tr>
<td>critical</td>
<td>Numerical severity 2. Indicates a critical condition</td>
</tr>
<tr>
<td>errors</td>
<td>Numerical severity 3. Indicates an error condition</td>
</tr>
<tr>
<td>warnings</td>
<td>Numerical severity 4. Indicates a warning condition</td>
</tr>
<tr>
<td>notification</td>
<td>Numerical severity 5. Indicates a normal but significant condition</td>
</tr>
<tr>
<td>informational</td>
<td>Numerical severity 6. Indicates a informational condition</td>
</tr>
<tr>
<td>debugging</td>
<td>Numerical severity 7. Debugging messages</td>
</tr>
<tr>
<td>dos</td>
<td>Identifies IP events as DoS events</td>
</tr>
<tr>
<td>ascend</td>
<td>Optional. Enables an ASCEND DoS check. Ascend routers listen on UDP port 9 for packets from Ascend's</td>
</tr>
<tr>
<td></td>
<td>Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.</td>
</tr>
<tr>
<td>broadcast-multicast-icmp</td>
<td>Optional. Detects broadcast or multicast ICMP packets as an attack</td>
</tr>
<tr>
<td>chargen</td>
<td>Optional. The Character Generation Protocol (chargen) is an IP suite service primarily used for testing</td>
</tr>
<tr>
<td></td>
<td>and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements.</td>
</tr>
<tr>
<td>fraggle</td>
<td>Optional. A Fraggle DoS attack checks for UDP packets to or from port 7 or 19</td>
</tr>
<tr>
<td>ftp-bounce</td>
<td>Optional. A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different</td>
</tr>
<tr>
<td></td>
<td>machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21),</td>
</tr>
<tr>
<td></td>
<td>another connection must open between the server and the client. To confirm, the PORT command has the</td>
</tr>
<tr>
<td></td>
<td>client specify an arbitrary destination machine and port for the data connection. This is exploited by</td>
</tr>
<tr>
<td></td>
<td>the attacker to gain access to a device that may not be the originating client.</td>
</tr>
<tr>
<td>invalid-protocol</td>
<td>Optional. Enables a check for invalid protocol number</td>
</tr>
</tbody>
</table>
### WiNG 5.8.1 CLI Reference Guide

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-ttl-zero</strong></td>
<td>Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)</td>
</tr>
<tr>
<td><strong>ipsproof</strong></td>
<td>Optional. Enables a check for IP spoofing DoS attack</td>
</tr>
<tr>
<td><strong>land</strong></td>
<td>Optional. A <em>Local Area Network Denial</em> (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device’s IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.</td>
</tr>
<tr>
<td><strong>option-route</strong></td>
<td>Optional. Enables an IP Option Record Route DoS check</td>
</tr>
<tr>
<td><strong>router-advt</strong></td>
<td>Optional. This is an attack, where a default route entry is added remotely to a device. This route entry is given preference, and thereby exposes an attack vector.</td>
</tr>
<tr>
<td><strong>router-solicit</strong></td>
<td>Optional. Router solicitation messages are sent to locate routers as a form of network scanning. This information can then be used to attack a device.</td>
</tr>
<tr>
<td><strong>smurf</strong></td>
<td>Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.</td>
</tr>
<tr>
<td><strong>snork</strong></td>
<td>Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU’s resources. This attack uses a UDP packet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.</td>
</tr>
<tr>
<td><strong>tcp-bad-sequence</strong></td>
<td>Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TCP connection</td>
</tr>
<tr>
<td><strong>tcp-fin-scan</strong></td>
<td>Optional. A FIN scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.</td>
</tr>
<tr>
<td><strong>tcp-intercept</strong></td>
<td>Optional. Prevents TCP intercept attacks by using TCP SYN cookies</td>
</tr>
<tr>
<td><strong>tcp-null-scan</strong></td>
<td>Optional. A TCP null scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports</td>
</tr>
<tr>
<td><strong>tcp-post-syn</strong></td>
<td>Optional. Enables a TCP post SYN DoS attack</td>
</tr>
<tr>
<td><strong>tcp-sequence-past-window</strong></td>
<td>Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP’s TCP stack which sends data past the window when conducting a selective ACK.</td>
</tr>
<tr>
<td><strong>tcp-xmas-scan</strong></td>
<td>Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.</td>
</tr>
<tr>
<td><strong>tcphdrfrag</strong></td>
<td>Optional. A DoS attack where the TCP header spans IP fragments</td>
</tr>
<tr>
<td><strong>twinge</strong></td>
<td>Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system</td>
</tr>
<tr>
<td><strong>udp-short-hdr</strong></td>
<td>Optional. Enables the identification of truncated UDP headers and UDP header length fields</td>
</tr>
<tr>
<td><strong>winnuke</strong></td>
<td>Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT, causing devices to crash with a blue screen</td>
</tr>
<tr>
<td><strong>drop-only</strong></td>
<td>Optional. Drops a packet without logging</td>
</tr>
</tbody>
</table>
- ip dos tcp-max-incomplete [high|low] <1-1000>

<table>
<thead>
<tr>
<th>dos</th>
<th>Identifies IP events as DoS events</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-max-incomplete</td>
<td>Sets the limits for the maximum number of incomplete TCP connections</td>
</tr>
<tr>
<td>high</td>
<td>Sets the upper limit for the maximum number of incomplete TCP connections</td>
</tr>
<tr>
<td>low</td>
<td>Sets the lower limit for the maximum number of incomplete TCP connections</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td>Sets the range limit from 1 - 1000 connections</td>
</tr>
</tbody>
</table>

- ip tcp adjust-mss <472-1460>

<table>
<thead>
<tr>
<th>tcp</th>
<th>Identifies and configures TCP events and configuration items</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjust-mss</td>
<td>Adjusts the TCP Maximum Segment Size (MSS). Use this option to adjust the MSS for TCP segments on the router.</td>
</tr>
<tr>
<td>&lt;472-1460&gt;</td>
<td>Sets the TCP MSS value from 472 - 1460 bytes. The default is 472 bytes.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>tcp</th>
<th>Identifies and configures TCP events and configuration items</th>
</tr>
</thead>
<tbody>
<tr>
<td>optimize-unnecessary-resends</td>
<td>Enables the validation of unnecessary TCP packets</td>
</tr>
<tr>
<td>recreate-flow-on-out-of-state-sync</td>
<td>Allows a TCP SYN packet to delete an old flow in TCP_FIN_FIN_STATE, and TCP_CLOSED_STATE states and create a new flow</td>
</tr>
<tr>
<td>validate-icmp-unreachable</td>
<td>Enables the validation of the sequence number in ICMP unreachable error packets, which abort an established TCP flow</td>
</tr>
<tr>
<td>validate-rst-ack-number</td>
<td>Enables the validation of the acknowledgment number in RST packets, which abort a TCP flow</td>
</tr>
<tr>
<td>validate-rst-seq-number</td>
<td>Enables the validation of the sequence number in RST packets, which abort an established TCP flow</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-rw-policy-test)#ip dos fraggle drop-only
rfs7000-37FABE(config-rw-policy-test)#ip dos tcp-max-incomplete high 600
rfs7000-37FABE(config-rw-policy-test)#ip dos tcp-max-incomplete low 60
rfs7000-37FABE(config-rw-policy-test)#ip dos tcp-sequence-past-window drop-only
```

```
rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
  ip dos fraggle drop-only
  ip dos tcp-sequence-past-window drop-only
  ip dos tcp-max-incomplete high 600
  ip dos tcp-max-incomplete low 60
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
  dhcp-offer-convert
dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

Related Commands

| no | Resets firewall policy IP components |
13.1.9 **ip-mac**

- **firewall-policy**

Defines an action based on the device IP MAC table, and also detects conflicts between IP addresses and MAC addresses.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ip-mac [conflict|routing]
```

```
ip-mac conflict drop-only
```

```
conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

```
ip-mac routing conflict drop-only
```

```
conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

**Parameters**

- ip-mac conflict drop-only

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conflict</td>
<td>Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default.</td>
</tr>
<tr>
<td>drop-only</td>
<td>Drops a packet without logging</td>
</tr>
</tbody>
</table>

- ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
| emergencies|errors|informational|notifications|warnings]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conflict</td>
<td>Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default.</td>
</tr>
<tr>
<td>log-and-drop</td>
<td>Logs the event and drops the packet. This is the default setting.</td>
</tr>
<tr>
<td>log-only</td>
<td>Logs the event only, the packet is not dropped</td>
</tr>
<tr>
<td>log-level</td>
<td>Configures the log level</td>
</tr>
<tr>
<td>&lt;0-7&gt;</td>
<td>Sets the numeric logging level</td>
</tr>
<tr>
<td>alerts</td>
<td>Numerical severity 1. Indicates a condition where immediate action is required</td>
</tr>
<tr>
<td>critical</td>
<td>Numerical severity 2. Indicates a critical condition</td>
</tr>
<tr>
<td>debugging</td>
<td>Numerical severity 7. Debugging messages</td>
</tr>
<tr>
<td>emergencies</td>
<td>Numerical severity 0. System is unusable</td>
</tr>
<tr>
<td>errors</td>
<td>Numerical severity 3. Indicates an error condition</td>
</tr>
<tr>
<td>informational</td>
<td>Numerical severity 6. Indicates a informational condition</td>
</tr>
<tr>
<td>notification</td>
<td>Numerical severity 5. Indicates a normal but significant condition</td>
</tr>
<tr>
<td>warnings</td>
<td>Numerical severity 4. Indicates a warning condition. This is the default setting</td>
</tr>
</tbody>
</table>
### **ip-mac routing conflict drop-only**

<table>
<thead>
<tr>
<th>routing</th>
<th>Enables IP/MAC routing conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>conflict</td>
<td>Defines the action performed when a routing table conflict is detected. This option is enabled by default.</td>
</tr>
<tr>
<td>drop-only</td>
<td>Drops a packet without logging</td>
</tr>
</tbody>
</table>

#### **Examples**

rfs7000-37FABE(config-rw-policy-test)#ip-mac conflict drop-only
rfs7000-37FABE(config-rw-policy-test)#ip-mac routing conflict log-and-drop log-level notifications
rfs7000-37FABE(config-fw-policy-test)#show context
default
firewall-policy test
  ip dos fraggle drop-only
  ip dos tcp-sequence-past-window drop-only
  ip dos tcp-max-incomplete high 600
  ip dos tcp-max-incomplete low 60
  ip-mac conflict drop-only
  ip-mac routing conflict log-only log-level notifications
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
  dhcp-offer-convert
dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables actions based on device IP MAC table, IP address, and MAC address</td>
</tr>
<tr>
<td></td>
<td>conflict detection</td>
</tr>
</tbody>
</table>
13.1.10 ipv6

**firewall-policy**

Configures IPv6 components on this firewall policy

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ipv6 [dos|duplicate-options|firewall|option|rewrite-flow-label|routing-type|
  strict-ext-hdr-check|unknown-options]

ipv6 dos {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility}
  [drop-only|log-and-drop|log-only]

ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|
  unknown-options] [drop-only|log-and-drop|log-only]

ipv6 option {endpoint-identification|network-service-access-point|router-alert|
  strict-hao-opt-alert|strict-padding} [drop-only|log-and-drop|log-only]

ipv6 [firewall enable|rewrite-flow-label]

**Parameters**

- **ipv6 dos** {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility}
  [drop-only|log-and-drop|log-only]

<table>
<thead>
<tr>
<th>dos</th>
<th>Identifies IPv6 events as DoS events</th>
</tr>
</thead>
<tbody>
<tr>
<td>hop-limit-zero</td>
<td>Optional. Enables checking of IPv6 hop limit field. If the IPv6 hop limit field is ZERO (0) it is considered as attack. This option is enabled by default.</td>
</tr>
<tr>
<td>multicast-icmpv6</td>
<td>Optional. Enables detection of multicast ICMPv6 traffic as attack. This option is applicable only to ICMPv6 Echo request or reply packets. This option is enabled by default.</td>
</tr>
<tr>
<td>tcp-intercept-mobility</td>
<td>Optional. Enables detection of IPv6 TCP packets with mobility option &quot;HAO(Home-Address-Option)&quot; or &quot;RH(Routing Header) type two&quot;. When enabled, this option also detects the &quot;don't generate TCP syn cookies&quot; for such packets. This option is enabled by default.</td>
</tr>
<tr>
<td>drop-only</td>
<td>This parameter is common to all of the above keywords. Drops all packets. Drops the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility).</td>
</tr>
<tr>
<td>log-and-drop</td>
<td>Logs the event and drops the packet. Drops the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility) and logs an event.</td>
</tr>
<tr>
<td>log-only</td>
<td>Logs the event only, the packet is not dropped. Does not drop the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility). But, an event is logged.</td>
</tr>
<tr>
<td>log-level</td>
<td>If selecting the &quot;log-and-drop&quot; and &quot;log-only&quot; action type, specify the log level. The options are:</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-7&gt; – Sets the numeric logging level</td>
</tr>
<tr>
<td></td>
<td>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</td>
</tr>
<tr>
<td></td>
<td>• critical – Numerical severity 2. Indicates a critical condition</td>
</tr>
<tr>
<td></td>
<td>• debugging – Numerical severity 7. Debugging messages</td>
</tr>
<tr>
<td></td>
<td>• emergencies – Numerical severity 0. System is unusable</td>
</tr>
<tr>
<td></td>
<td>• errors – Numerical severity 3. Indicates an error condition</td>
</tr>
<tr>
<td></td>
<td>• informational – Numerical severity 6. Indicates an informational condition</td>
</tr>
<tr>
<td></td>
<td>• notifications – Numerical severity 5. Indicates a normal but significant condition</td>
</tr>
<tr>
<td></td>
<td>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</td>
</tr>
</tbody>
</table>

- ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-options] [drop-only|log-and-drop|log-only]

<table>
<thead>
<tr>
<th>duplicate-options</th>
<th>Enables handling of duplicate options in hop-by-hop and destination option extension headers. This configuration excludes HAO handling. This option is enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-type [one</td>
<td>two]</td>
</tr>
<tr>
<td></td>
<td>• one – Routing Type 1(Nimrod routing). This option is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• two – Routing Type 2(Mobile IP). This option is disabled by default.</td>
</tr>
<tr>
<td>strict-ext-hdr-check</td>
<td>Enables strict checking for out of order and number of occurrences of extension header. This option is enabled by default.</td>
</tr>
<tr>
<td>unknown-options</td>
<td>Enables handling unknown options in hop-by-hop and destination option extension headers. This option is enabled by default.</td>
</tr>
<tr>
<td>drop-only</td>
<td>This parameter is common to all of the above keywords.</td>
</tr>
<tr>
<td></td>
<td>Drops all packets. Drops the packet if matching any of the above specified types.</td>
</tr>
<tr>
<td>log-and-drop</td>
<td>Logs the event and drops the packet. Drops the packet, if matching any of the above specified types, and logs an event.</td>
</tr>
<tr>
<td>log-only</td>
<td>Logs the event only, the packet is not dropped. Does not drop the packet, if matching any of the above specified types. But an event is logged.</td>
</tr>
<tr>
<td>log-level</td>
<td>If selecting the &quot;log-and-drop&quot; and &quot;log-only&quot; action type, specify the log level. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-7&gt; – Sets the numeric logging level</td>
</tr>
<tr>
<td></td>
<td>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</td>
</tr>
<tr>
<td></td>
<td>• critical – Numerical severity 2. Indicates a critical condition</td>
</tr>
<tr>
<td></td>
<td>• debugging – Numerical severity 7. Debugging messages</td>
</tr>
<tr>
<td></td>
<td>• emergencies – Numerical severity 0. System is unusable</td>
</tr>
<tr>
<td></td>
<td>• errors – Numerical severity 3. Indicates an error condition</td>
</tr>
<tr>
<td></td>
<td>• informational – Numerical severity 6. Indicates an informational condition</td>
</tr>
<tr>
<td></td>
<td>• notifications – Numerical severity 5. Indicates a normal but significant condition</td>
</tr>
<tr>
<td></td>
<td>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</td>
</tr>
</tbody>
</table>


**ipv6 option** {endpoint-identification|network-service-access-point|router-alert|strict-hao-opt-alert|strict-padding} [drop-only|log-and-drop|log-only]

<table>
<thead>
<tr>
<th>option</th>
<th>Enables checking for the following ipv6 extension header options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• End point identification option (disabled by default)</td>
</tr>
<tr>
<td></td>
<td>• Network service access point address option (disabled by default)</td>
</tr>
<tr>
<td></td>
<td>• Router alert option (disabled by default)</td>
</tr>
<tr>
<td></td>
<td>• Home address option in destination option extension header (enabled by default)</td>
</tr>
<tr>
<td></td>
<td>• Pad1 and PadN options validating (enabled by default)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All of these are optional parameters. If no option is specified, the system enables checks as per the default values.</td>
</tr>
</tbody>
</table>

| drop-only | This parameter is common to all of the above keywords. Drops all packets. Drops the packet if matching any of the above specified “option” types. |
| log-and-drop | Logs the event and drops the packet. Drops the packet, if matching any of the above specified “option” types, and logs an event. |
| log-only | Logs the event only, the packet is not dropped. Does not drop the packet, if matching any of the above specified “option” types. But an event is logged. |

| log-level | If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: |
|           | • <0-7> – Sets the numeric logging level |
|           | • alerts – Numerical severity 1. Indicates a condition where immediate action is required |
|           | • critical – Numerical severity 2. Indicates a critical condition |
|           | • debugging – Numerical severity 7. Debugging messages |
|           | • emergencies – Numerical severity 0. System is unusable |
|           | • errors – Numerical severity 3. Indicates an error condition |
|           | • informational – Numerical severity 6. Indicates a informational condition |
|           | • notifications – Numerical severity 5. Indicates a normal but significant condition |
|           | • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting. |

**ipv6 [firewall enable|rewrite-flow-label]**

| firewall enable | Enables IPv6 firewall. This option is enabled by default. |
| rewrite-flow-label | Rewrites the IPv6 flow label field of every packet. This option is disabled by default. |

**Examples**

```
nx4500-5CFA2B(config-fw-policy-test)#ipv6 dos hop-limit-zero drop-only
nx4500-5CFA2B(config-fw-policy-test)#ipv6 routing-type two log-and-drop log-level warnings
nx4500-5CFA2B(config-fw-policy-test)#show context firewall-policy test
no ip dos tcp-sequence-past-window
ipv6 routing-type two log-and-drop log-level warnings
ipv6 dos hop-limit-zero drop-only
nx4500-5CFA2B(config-fw-policy-test)#
```

**Related Commands**

```
no
```

Resets this firewall policy’s IPv6 components
### 13.1.11 ipv6-mac

#### firewall-policy

Defines an action based on conflicts detected in a device’s IPv6 and MAC addresses.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
ipv6-mac [conflict|routing]
ipv6-mac conflict [drop-only|log-and-drop|log-only]
ipv6-mac routing conflict [drop-only|log-and-drop|log-only]
```

#### Parameters

- `ipv6-mac conflict [drop-only|log-and-drop|log-only]`
  - `conflict` Enables detection of conflict between a device’s IPv6 and MAC addresses. This option is enabled by default. This command also specifies the action to be performed when a such a conflict is detected. The options are: drop-only, log-and-drop, and log-only
  - `drop-only` Drops a packet (with conflicting IPv6 and MAC address) without logging
  - `log-and-drop` Logs the event and drops the packet. This is the default setting.
  - `log-only` Logs the event only, the packet is not dropped
  - `log-level` If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are:
    - `<0-7>` – Sets the numeric logging level
    - `alerts` – Numerical severity 1. Indicates a condition where immediate action is required
    - `critical` – Numerical severity 2. Indicates a critical condition
    - `debugging` – Numerical severity 7. Debugging messages
    - `emergencies` – Numerical severity 0. System is unusable
    - `errors` – Numerical severity 3. Indicates an error condition
    - `informational` – Numerical severity 6. Indicates a informational condition
    - `notifications` – Numerical severity 5. Indicates a normal but significant condition
    - `warnings` – Numerical severity 4. Indicates a warning condition. This is the default setting.

- `ipv6-mac routing conflict [drop-only|log-and-drop|log-only]`
  - `routing conflict` Enables detection of conflict between the next-hop’s IPv6 and MAC addresses. This option is enabled by default. This command also specifies the action to be performed when a such a conflict is detected. The options are: drop-only, log-and-drop, and log-only
  - `drop-only` Drops a packet (with conflicting next-hop IPv6 and MAC addresses) without logging
  - `log-and-drop` Logs the event and drops the packet. This is the default setting.
FIREWALL-POLICY 13-27

<table>
<thead>
<tr>
<th>log-only</th>
<th>Logs the event only, the packet is not dropped</th>
</tr>
</thead>
</table>
| **log-level** | If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are:  
| | • <0-7> – Sets the numeric logging level  
| | • alerts – Numerical severity 1. Indicates a condition where immediate action is required  
| | • critical – Numerical severity 2. Indicates a critical condition  
| | • debugging – Numerical severity 7. Debugging messages  
| | • emergencies – Numerical severity 0. System is unusable  
| | • errors – Numerical severity 3. Indicates an error condition  
| | • informational – Numerical severity 6. Indicates an informational condition  
| | • notifications – Numerical severity 5. Indicates a normal but significant condition  
| | • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting. |

**Examples**

nx4500-5CFA2B(config-fw-policy-test)#ipv6-mac routing conflict drop-only

nx4500-5CFA2B(config-fw-policy-test)#show context
firewall-policy test
  no ip dos tcp-sequence-past-window
  ipv6 routing-type two log-and-drop log-level warnings
  ipv6 dos hop-limit-zero drop-only
  ipv6-mac routing conflict drop-only
nx4500-5CFA2B(config-fw-policy-test)#

**Related Commands**

| **no** | Disables actions based on device IPv6 MAC table, next-hop’s IPv6 and MAC address conflict detection |
13.1.12 logging

`firewall-policy`

Configures enhanced firewall logging

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`logging [icmp-packet-drop|malformed-packet-drop|verbose]`

`logging verbose`

`logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]`

**Parameters**

- `logging verbose`
- `logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]`

<table>
<thead>
<tr>
<th>logging</th>
<th>Configures enhanced firewall logging. This option is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>verbose</td>
<td>Enables verbose logging</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>logging</th>
<th>Configures enhanced firewall logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-packet-drop</td>
<td>Drops ICMP (ICMPv4 and ICMPv6) packets that do not pass sanity checks. The default is none.</td>
</tr>
<tr>
<td>malformed-packet-drop</td>
<td>Drops raw IP (IPv4 and IPv6) packets that do not pass sanity checks. The default is none.</td>
</tr>
<tr>
<td>all</td>
<td>Logs all messages</td>
</tr>
<tr>
<td>rate-limited</td>
<td>Enables rate-limited logging. This option sets the rate limit for log messages to one message every 20 seconds.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37PABE(config-rw-policy-test)#logging verbose
rfs7000-37PABE(config-rw-policy-test)#logging icmp-packet-drop rate-limited
rfs7000-37PABE(config-rw-policy-test)#logging malformed-packet-drop all
rfs7000-37PABE(config-fw-policy-test)#show context
firewall-policy test
  ip dos fraggle drop-only
  ip dos tcp-sequence-past-window drop-only
  ip dos tcp-max-incomplete high 600
  ip dos tcp-max-incomplete low 60
  ip-mac conflict drop-only
  ip-mac routing conflict log-only log-level notifications
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
  dhcp-offer-convert
  logging icmp-packet-drop rate-limited
  logging malformed-packet-drop all
  logging verbose
dns-snoop entry-timeout 35
rfs7000-37PABE(config-fw-policy-test)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables enhanced firewall logging</td>
</tr>
</tbody>
</table>
13.1.13 no

Negates a command or sets the default for firewall policy commands

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
no [acl-logging|alg|clamp|dhcp-offer-convert|dns-snoop|firewall|flow|ip|ip-mac|ipv6|ipv6-mac|logging|proxy-arp|stateful-packet-inspection-l2|storm-control|virtual-defragmentation]
```

```
no [acl-logging|dhcp-offer-convert|proxy-arp|stateful-packet-inspection-l2]
```

no alg [dns|facetime|ftp|pptp|sccp|sip|tftp]

no clamp tcp-mss

no dns-snoop entry-timeout

no firewall enable

no flow dhcp stateful

no flow timeout [icmp|other|udp]

no flow timeout tcp [closed-wait|established|reset|setup|stateless-fin-or-reset|stateless-general]

```
```

no tcp [adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]

```
no ip tcp [adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

no ip-mac conflict

no ipv6 [duplicate-options|firewall|option|rewrite-flow-label|routing-type|strict-ext-hdr-check|unknown-options]

```
o ipv6 dos {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility}
o ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-options]
o ipv6 option {endpoint-identification|network-service-access-point|router-alert|strict-hao-opt-alert|strict-padding}
o ipv6 [firewall enable|rewrite-flow-label]
```

no ip-mac routing conflict

```
no ipv6 dos {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility}
```

```
no ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-options]
```

```
o ipv6 option {endpoint-identification|network-service-access-point|router-alert|strict-hao-opt-alert|strict-padding}
```

no ipv6 [firewall enable|rewrite-flow-label]

```
```

no logging [icmp-packet-drop|verbose|malformed-packet-drop]

```
```

no storm-control [arp|broadcast|multicast|unicast] {fe <1-4>|ge <1-8>|log|port-channel <1-8>|up1|wlan <WLAN-NAME>}

no virtual-defragmentation {maximum-fragments-per-datagram|minimum-first-fragment-length|maximum-defragmentation-per-host|timeout}

Parameters

- no <PARAMETERS> Negates a command or sets the default for firewall policy commands.
Examples

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
  ip dos fraggle drop-only
  no ip dos tcp-sequence-past-window
  ip dos tcp-max-incomplete high 600
  ip dos tcp-max-incomplete low 60
  storm-control broadcast level 20000 ge 4
  storm-control arp log warnings
  ip-mac conflict drop-only
  ip-mac routing conflict log-and-drop log-level notifications
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
  dhcp-offer-convert
  logging icmp-packet-drop rate-limited
  logging malformed-packet-drop all
  logging verbose
  dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#

rfs7000-37FABE(config-fw-policy-test)#no ip dos fraggle
rfs7000-37FABE(config-fw-policy-test)#no storm-control arp log
rfs7000-37FABE(config-fw-policy-test)#no dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-test)#no logging malformed-packet-drop

rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
  no ip dos fraggle
  no ip dos tcp-sequence-past-window
  ip dos tcp-max-incomplete high 600
  ip dos tcp-max-incomplete low 60
  storm-control broadcast level 20000 ge 4
  storm-control arp log none
  ip-mac conflict drop-only
  ip-mac routing conflict log-and-drop log-level notifications
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
  logging icmp-packet-drop rate-limited
  logging verbose
  dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
13.1.14 proxy-arp

firewall-policy

Enables the generation of ARP responses on behalf of another device. Proxy ARP allows the Firewall to handle ARP routing requests for devices behind the firewall. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
proxy-arp

**Parameters**
None

**Examples**
rfs7000-37FABE(config-fw-policy-test)#proxy-arp
rfs7000-37FABE(config-fw-policy-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the generation of ARP responses on behalf of another device</td>
</tr>
</tbody>
</table>
13.1.15 proxy-nd

- **firewall-policy**

  Enables generation of ND responses (for IPv6) on behalf of another device

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`proxy-nd`

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-fw-policy-fw1)#proxy-nd
nx9500-6C8809(config-fw-policy-fw1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables the generation of ND responses on behalf of another device</td>
</tr>
</tbody>
</table>
13.1.16 **stateful-packet-inspection-l2**

```
  firewall-policy
```

Enables layer 2 firewall stateful packet inspection. When enabled, allows stateful packet inspection for RF Domain manager routed interfaces within the layer 2 firewall. This option is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
stateful-packet-inspection-l2
```

**Parameters**
None

**Examples**
```
rfs7000-37FABE(config-fw-policy-test)#stateful-packet-inspection-l2
rfs7000-37FABE(config-fw-policy-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables stateful packet inspection in a layer 2 firewall</td>
</tr>
</tbody>
</table>
13.1.17 storm-control

*firewall-policy*

Enables storm control on the firewall policy

Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the RF Domain manager interface.

Storm control limits multicast, unicast and broadcast frames accepted and forwarded by a device. Messages are logged based on their severity level.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
storm-control [arp|broadcast|multicast|unicast] level <1-1000000> 
storm-control [arp|broadcast|multicast|unicast] log [alerts|critical|debugging|emergencies|errors|informational|none|notifications|warnings]
```

**Parameters**
- **arp** Configures storm control for ARP packets
- **broadcast** Configures storm control for broadcast packets
- **multicast** Configures storm control for multicast packets
- **unicast** Configures storm control for unicast packets
- **level <1-1000000>** Configures the allowed number of packets received per second before storm control begins
  - `<1-1000000>` – Sets the number of packets received per second
- **fe <1-4>** Sets the FastEthernet port for storm control from 1 - 4
- **ge <1-8>** Sets the GigabitEthernet port for storm control from 1 - 8
  - **Note:** For the NX45XX and NX65XX service platforms, the GE port range is 1 - 24.
- **port-channel <1-8>** Sets the port channel for storm control from 1- 8
- **up1** Sets the uplink interface
  - **Note:** For the NX45XX and NX65XX service platforms, the uplink interface range is 1 - 2.
- **wlan <WLAN-NAME>** Configures the WLAN
  - `<WLAN-NAME>` – Sets the WLAN ID for the storm control configuration
storm-control [arp|bcast|multicast|unicast] log [<0-7>|alerts|critical|debugging|emergencies|errors|informational|none|notifications|warnings]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Configures storm control for ARP packets</td>
</tr>
<tr>
<td>broadcast</td>
<td>Configures storm control for broadcast packets</td>
</tr>
<tr>
<td>multicast</td>
<td>Configures storm control for multicast packets</td>
</tr>
<tr>
<td>unicast</td>
<td>Configures storm control for unicast packets</td>
</tr>
<tr>
<td>log</td>
<td>Configures the storm control log level for storm control events</td>
</tr>
<tr>
<td>&lt;0-7&gt;</td>
<td>Sets the numeric logging level from 0 - 7</td>
</tr>
<tr>
<td>alerts</td>
<td>Numerical severity 1. Indicates a condition where immediate action is required</td>
</tr>
<tr>
<td>critical</td>
<td>Numerical severity 2. Indicates a critical condition</td>
</tr>
<tr>
<td>debugging</td>
<td>Numerical severity 7. Debugging messages</td>
</tr>
<tr>
<td>emergencies</td>
<td>Numerical severity 0. System is unusable</td>
</tr>
<tr>
<td>errors</td>
<td>Numerical severity 3. Indicates an error condition</td>
</tr>
<tr>
<td>informational</td>
<td>Numerical severity 6. Indicates a informational condition</td>
</tr>
<tr>
<td>none</td>
<td>Disables storm control logging</td>
</tr>
<tr>
<td>notification</td>
<td>Numerical severity 5. Indicates a normal but significant condition</td>
</tr>
<tr>
<td>warnings</td>
<td>Numerical severity 4. Indicates a warning condition. This is the default setting.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-fw-policy-test)#storm-control arp log warning
rfs7000-37FABE(config-fw-policy-test)#storm-control broadcast level 20000 ge 4
rfs7000-37FABE(config-fw-policy-test)#show context
firewall-policy test
  ip dos fraggle drop-only
  no ip dos tcp-sequence-past-window
  ip dos tcp-max-incomplete high 600
  ip dos tcp-max-incomplete low 60
  storm-control broadcast level 20000 ge 4
  storm-control arp log warnings
  ip-mac conflict drop-only
  ip-mac routing conflict log-and-drop log-level notifications
  flow timeout icmp 16000
  flow timeout udp 10000
  flow timeout tcp established 1500
  flow timeout other 16000
  dhcp-offer-convert
  logging icmp-packet-drop rate-limited
  logging malformed-packet-drop all
  logging verbose
  dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#

Related Commands

no | Disables storm control limits on multicast, unicast, and broadcast frames accepted and forwarded by a device
13.1.18 virtual-defragmentation

firewall-policy

Enables the virtual defragmentation of IPv4 and IPv6 packets. This parameter is required for optimal firewall functionality and is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>|timeout <1-60}]
```

Parameters

- `virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>|timeout <1-60>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| maximum-defragmentation-per-host `<1-16384>` | Optional. Configures the maximum number of active defragmentations allowed per host before it is dropped (applicable to IPv4 and IPv6 packets)  
  - `<1-16384>` – Sets a value from 1 - 16384. The default is 8. |
| maximum-fragments-per-datagram `<2-8129>` | Optional. Configures the maximum number of fragments allowed in a datagram before it is dropped (applicable to IPv4 and IPv6 packets)  
  - `<2-8129>` – Sets a value from 2 - 8129. The default is 140. |
| minimum-first-fragment-length `<8-1500>` | Optional. Defines the minimum length required for the first fragment (applicable to IPv4 and IPv6 packets)  
  - `<8-1500>` – Sets a value from 8 - 1500 bytes. The default is 8 bytes. |
| timeout `<1-60>` | Optional. Configures a virtual defragmentation timeout, in seconds, applicable to both IPv4 and IPv6 packets  
  - `<1-60>` – Specify a value from 1 - 60 seconds. The default is 1 second. |

Examples

```
rfs7000-37FABE(config-fw-policy-test)#virtual-defragmentation maximum-fragments-per-datagram 10
rfs7000-37FABE(config-fw-policy-test)#virtual-defragmentation minimum-first-fragment-length 100
```

Related Commands

- `no` | Resets values or disables virtual defragmentation settings |
This chapter summarizes MiNT policy commands in the CLI command structure.

All communication using the MiNT transport layer can be optionally secured. This includes confidentiality, integrity and authentication of all communications. In addition, a device can be configured to communicate over MiNT with other devices authorized by an administrator.

Use the (config) instance to configure mint-policy related configuration commands. To navigate to the config MiNT policy instance, use the following command:

```
<DEVICE>(config)#mint-policy global-default
```

```
rfs7000-37FABE(config-mint-policy-global-default)#?
```

Mint Policy Mode commands:

- `level` Mint routing level
- `mtu` Configure the global Mint MTU
- `no` Negate a command or set its defaults
- `router` Mint router
- `udp` Configure mint UDP/IP encapsulation
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-mint-policy-global-default)#
```

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
14.1 mint-policy

The following table summarizes MiNT policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Configures the MiNT routing level</td>
<td>page 14-3</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the global MiNT MTU</td>
<td>page 14-4</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 14-7</td>
</tr>
<tr>
<td>router</td>
<td>Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)</td>
<td>page 14-5</td>
</tr>
<tr>
<td>udp</td>
<td>Configures the MiNT UDP/IP encapsulation parameters</td>
<td>page 14-6</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
14.1.1 level

mint-policy

Configures the global MiNT routing level

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
level 2 area-id <1-16777215>

Parameters
- level 2 area-id <1-16777215>

| level 2 | Configures level 2 inter-site MiNT routing |
| area-id | Configures the routing area identifier |
| <1-16777215> | • <1-16777215> – Specify a value from 1 - 16777215. The level 2 area ID is the global MiNT area identifier. This area identifier separates two overlapping MiNT networks. Configure the level 2 area ID only if there are two MiNT networks sharing the same packet broadcast domain. |

Examples
rfs7000-37FABE(config-mint-policy-global-default)#level 2 area-id 2000
rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
level 2 area-id 2000
rfs7000-37FABE(config-mint-policy-global-default)#

Related Commands
- no Disables level 2 MiNT packet routing (inter-site packet routing)
14.1.2 mtu

▶ mint-policy

Configures global MiNT Multiple Transmission Unit (MTU). Use this command to specify the maximum packet size, in bytes, for MiNT routing. Higher the MTU values, greater is the network efficiency. The user data per packet increases, while protocol overheads, such as headers or underlying per-packet delays remain the same.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

mtu <900-1500>

Parameters

- mtu <900-1500>

| <900-1500> | Specifies the maximum packet size from 900 - 1500 bytes. The maximum packet size specified is rounded down to a value using the following formula: 4 + a multiple of 8. The MTU setting specifies the maximum packet size used for MiNT packets. Larger packets are fragmented to fit within the specified packet size limit. You may want to configure this parameter if the MiNT backhaul network requires or recommends smaller packet sizes. The default value is 1500 bytes. |

Examples

rfs7000-37FABE(config-mint-policy-global-default)#mtu 1000
rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
  mtu 996
  level 2 area-id 2
rfs7000-37FABE(config-mint-policy-global-default)#

Related Commands

no | Reverts the configured MiNT MTU value to its default (1500 bytes)
   | Negates the configured maximum packet size for MiNT routing
14.1.3 router

Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXT VLAN)

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
router packet priority <0-7>
```

Parameters

- `router packet priority <0-7>`

Examples

```
rfs4000-229D58(config-mint-policy-global-default)#router packet priority 4
rfs4000-229D58(config-mint-policy-global-default)#show context mint-policy global-default router packet priority 4
rfs4000-229D58(config-mint-policy-global-default)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Reverts the MiNT router packet priority to default (5)</td>
</tr>
</tbody>
</table>
14.1.4 udp

- mint-policy

Configures MiNT UDP/IP encapsulation parameters. Use this command to configure the default UDP port used for MiNT control packet encapsulation.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
udp port <2-65534>

Parameters
- udp port <2-65534>

Examples
rfs7000-37FABE(config-mint-policy-global-default)#udp port 1024
rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
  udp port 1024
  mtu 996
  level 2 area-id 2000
  sign-unknown-device
  security-level control-and-data
  rejoin-timeout 1000
rfs7000-37FABE(config-mint-policy-global-default)#

Related Commands

no

Reverts MiNT UDP/IP encapsulation to its default
### 14.1.5 no

Negates a command or reverts values to their default. When used in the config MiNT policy mode, the *no* command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [level|mtu|router|udp]
```

- `no level 2 area-id`
- `no mtu`
- `no router packet priority`
- `no udp port <LINE-SINK>`

**Parameters**

- `no <PARAMETERS>`

| no <PARAMETERS> | The *no* command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings. |

**Examples**

The following example shows the global Mint Policy parameters before the ‘*no*’ commands are executed:

```plaintext
rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
  udp port 1024
  mtu 996
  level 2 area-id 2000
  sign-unknown-device
  security-level control-and-data
  rejoin-timeout 1000
rfs7000-37FABE(config-mint-policy-global-default)#
```

The following example shows the global Mint Policy parameters after the ‘*no*’ commands are executed:

```plaintext
rfs7000-37FABE(config-mint-policy-global-default)#no level 2 area-id
rfs7000-37FABE(config-mint-policy-global-default)#no mtu
rfs7000-37FABE(config-mint-policy-global-default)#no udp port

rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
  sign-unknown-device
  security-level control-and-data
  rejoin-timeout 1000
rfs7000-37FABE(config-mint-policy-global-default)#
```
CHAPTER 15
MANAGEMENT-POLICY

This chapter summarizes management policy commands in the CLI command structure.
A management policy contains configuration elements for managing a device, such as access control, SNMP, admin user credentials, and roles.

A controller (wireless controller, access point, or service platform) uses mechanisms to allow or deny device access to separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled or disabled as required for unique policies. The management access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can do the following:

- Restrict SNMP, CLI and Web UI access to specific hosts or subnets
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices
- Provide authentication for management users
- Apply access restrictions and permissions to management users

Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.

Access Points utilize a single management access policy, so ensure all the intended administrative roles, permissions, authentication and SNMP settings are correctly set. If an access point is functioning as a virtual controller AP, these are the access settings used by adopted access points of the same model as the virtual controller AP.

It is recommended to disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.

Use the (config) instance to configure a management policy. To navigate to the config management policy instance, use the following commands:

<DEVICE>(config)#management-policy <POLICY-NAME>

To commit a management-policy, the policy must have at least one admin user account configured.
<DEVICE>(config-management-policy-<POLICY-NAME>)#user admin password 0 test role superuser access all
<DEVICE>(config-management-policy-<POLICY-NAME>)#

<DEVICE>(config-management-policy-<POLICY-NAME>)#?
Management Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-login</td>
<td>Set authentication for logins</td>
</tr>
<tr>
<td>banner</td>
<td>Define a login banner</td>
</tr>
<tr>
<td>ftp</td>
<td>Enable FTP server</td>
</tr>
<tr>
<td>http</td>
<td>Hyper Text Terminal Protocol (HTTP)</td>
</tr>
<tr>
<td>https</td>
<td>Secure HTTP</td>
</tr>
<tr>
<td>idle-session-timeout</td>
<td>Configure idle timeout for a configuration session (GUI or CLI)</td>
</tr>
<tr>
<td>ipv6</td>
<td>IPv6 Protocol</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>privilege-mode-password</td>
<td>Set the password for entering CLI privilege mode</td>
</tr>
<tr>
<td>restrict-access</td>
<td>Restrict management access to the device</td>
</tr>
<tr>
<td>snmp-server</td>
<td>SNMP</td>
</tr>
<tr>
<td>ssh</td>
<td>Enable ssh</td>
</tr>
<tr>
<td>t5</td>
<td>T5 configuration</td>
</tr>
<tr>
<td>telnet</td>
<td>Enable telnet</td>
</tr>
<tr>
<td>user</td>
<td>Add a user account</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

<DEVICE>(config-management-policy-<POLICY-NAME>)#

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
15.1 management-policy

The following table summarizes management policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-login</td>
<td>Configures login authentication settings</td>
<td>page 15-4</td>
</tr>
<tr>
<td>banner</td>
<td>Configures the <em>message of the day</em> (motd) text</td>
<td>page 15-6</td>
</tr>
<tr>
<td>ftp</td>
<td>Enables FTP on this management policy</td>
<td>page 15-7</td>
</tr>
<tr>
<td>http</td>
<td>Enables HTTP on this management policy</td>
<td>page 15-9</td>
</tr>
<tr>
<td>https</td>
<td>Enables HTTPS on this management policy</td>
<td>page 15-10</td>
</tr>
<tr>
<td>idle-session-timeout</td>
<td>Sets the interval after which an idle session is terminated</td>
<td>page 15-11</td>
</tr>
<tr>
<td>ipv6</td>
<td>Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively</td>
<td>page 15-12</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets this management policy’s settings</td>
<td>page 15-14</td>
</tr>
<tr>
<td>privilege-mode-password</td>
<td>Configures the CLI's privilege mode access password</td>
<td>page 15-16</td>
</tr>
<tr>
<td>restrict-access</td>
<td>Restricts management access to a set of hosts or subnets</td>
<td>page 15-17</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Sets the SNMP server settings on this management policy</td>
<td>page 15-19</td>
</tr>
<tr>
<td>ssh</td>
<td>Enables SSH on this management policy</td>
<td>page 15-23</td>
</tr>
<tr>
<td>t5</td>
<td>Configures SNMP server settings for T5 devices on this management policy. This command is available only RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, and NX9000 platforms.</td>
<td>page 15-24</td>
</tr>
<tr>
<td>telnet</td>
<td>Enables Telnet on this management policy</td>
<td>page 15-26</td>
</tr>
<tr>
<td>user</td>
<td>Creates a new user account</td>
<td>page 15-27</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands to troubleshoot or debug <em>(config-if)</em> instance configurations</td>
<td>page 15-29</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, **COMMON COMMANDS**.
### 15.1.1 `aaa-login` management-policy

Configures Authentication, Authorization and Accounting (AAA) authentication mode used with this management policy. The different modes are: local authentication and external RADIUS server authentication.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
aaa-login [local|radius|tacacs]
```

```
aaa-login local
```

```
aaa-login radius [external|fallback|policy]
```

```
aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]
```

```
aaa-login tacacs [accounting|authentication|authorization|fallback|policy]
```

```
aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-TACACS-POLICY-NAME>]
```

#### Parameters

- **local**
  - Sets local as the preferred authentication mode. Local authentication uses the local username database to authenticate a user.
  - **Note:** The AP6511 and AP6521 platforms do not support local RADIUS resource.

- **radius**
  - Configures the RADIUS server parameters
  - **Note:** If local authentication is disabled, use this command to specify if the RADIUS server used is external, fallback, or specified by a AAA policy.

- **external**
  - Configures external RADIUS server as the preferred authentication mode

- **fallback**
  - Configures RADIUS server authentication as the primary authentication mode
  - When RADIUS server authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.

- **policy <AAA-POLICY-NAME>**
  - Associates a specified AAA policy with this management policy. The AAA policy determines if a client is granted access to the network.
  - **Note:** For more information on configuring AAA policy, see [AAA-POLICY].

- **tacacs**
  - Configures Terminal Access Control Access-Control System (TACACS) server parameters

- **accounting**
  - Configures TACACS accounting

- **authentication**
  - Configures TACACS authentication

---
Usage Guidelines
Use AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

Examples
rfs7000-37FABE(config-management-policy-test)#aaa-login radius external
rfs7000-37FABE(config-management-policy-test)#aaa-login radius policy test
rfs7000-37FABE(config-management-policy-test)#show context management-policy test
  http server
  no ssh
  aaa-login radius external
  aaa-login radius policy test
rfs7000-37FABE(config-management-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the TACACS server settings</td>
</tr>
</tbody>
</table>
15.1.2 banner

management-policy

Configures the message of the day (motd) text. This text is displayed at login to clients connecting through Telnet or SSH.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

banner motd <LINE>

Parameters

- banner motd <LINE>

<table>
<thead>
<tr>
<th>motd &lt;LINE&gt;</th>
<th>Sets the motd banner</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LINE&gt; – Enter the message string. The message string should not exceed 255 characters.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-management-policy-test)#banner motd "Have a Good Day"

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  http server
  no ssh
  aaa-login radius external
  aaa-login radius policy test
  banner motd "Have a Good Day"

rfs7000-37FABE(config-management-policy-test)#

Related Commands

| no | Removes the motd banner |
### 15.1.3 ftp

**management-policy**

Enables File Transfer Protocol (FTP) on this management policy. FTP is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally. FTP access is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
ftp {password|rootdir|username}
ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}  
ftp {rootdir <DIR>}
ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}
```

**Parameters**

- **ftp password**
  - Optional. Configures the FTP server password
  - `1 <ENCRYPTED-PASSWORD>`
    - Configures an encrypted password. Use this option when copy pasting the password from another device.
    - `<ENCRYPTED-PASSWORD>` – Specify the password. The password should not exceed 63 characters in length.
  - `<PASSWORD>`
    - Configures a clear text password

- **ftp rootdir <DIR>**
  - Optional. Configures the root directory for FTP logins
  - `<DIR>` – Specify the root directory path. By default the root directory is set to flash: /

- **ftp username <USERNAME>**
  - Optional. Configures a new user account on the FTP server. The FTP user file lists users with FTP server access.
  - `<USERNAME>` – Specify the username. The username should not exceed 32 characters in length.
  - `password 1 [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]`
    - Configures an encrypted password
    - `<ENCRYPTED-PASSWORD>` – Specifies an encrypted password (use this option if copy pasting from another device). The password should not exceed 63 characters in length.
    - `<PASSWORD>` – Configures a clear text password

- **rootdir <DIR>**
  - After specifying the password, configure the FTP root directory.
  - `rootdir <DIR>` – Configures the root directory for FTP logins. Specify the root directory path.
Usage Guidelines
The string size of an encrypted password (option 1, password is encrypted with a SHA1 algorithm) must be exactly 40 characters.

Examples
rfs7000-37FABE(config-management-policy-test)#ftp username superuser password test@123 rootdir dir
rfs7000-37FABE(config-management-policy-test)#show context management-policy test
http server
ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables FTP and its settings, such as the server password, root directory, and users</td>
</tr>
</tbody>
</table>
15.1.4 http

*management-policy*

Enables *Hyper Text Transport Protocol* (HTTP) on this management policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
http server
```

**Parameters**

- `http server`

| http server | Enables HTTP on this management policy. HTTP provides limited authentication and no encryption. |

**Examples**

```
rfs7000-37FABE(config-management-policy-test)#http server
```

```
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  http server
  ftp username superuser password 1
  f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir no ssh
  aaa-login radius external
  aaa-login radius policy test
  banner motd "Have a Good Day"
rfs7000-37FABE(config-management-policy-test)#
```

**Related Commands**

| no | Disables HTTP on this management policy |
### 15.1.5 https

**management-policy**

Enables Hyper Text Transport Protocol Secure (HTTPS) on this management policy.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`https server`

**Parameters**

- `https server`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>https server</code></td>
<td>Enables HTTPS on this management policy. HTTPS provides both authentication and data encryption as opposed to just authentication.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-management-policy-test)#https server
rfs7000-37FABE(config-management-policy-test)#show context
rfs7000-37FABE(config-management-policy-test)<(config-context)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables HTTPS on this management policy</td>
</tr>
</tbody>
</table>
### 15.1.6 idle-session-timeout

> **management-policy**

Configures a session’s idle timeout. An idle session is automatically terminated after the specified interval is exceeded.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
idle-session-timeout <1-4320>
```

**Parameters**

- `idle-session-timeout <1-4320>`

**Examples**

```bash
rfs7000-37FABE(config-management-policy-test)#idle-session-timeout 100
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  http server
  https server
  ftp username superuser password 1
  f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
  no ssh
  aaa-login radius external
  aaa-login radius policy test
  **idle-session-timeout 100**
  banner motd "Have a Good Day"
```

**Related Commands**

- `no` | Removes the configured idle session timeout value
15.1.7 ipv6

- management-policy

Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ipv6 restrict-access [host|ipv6-access-list|subnet]

ipv6 restrict-access host <IPv6> {log|subnet}
ipv6 restrict-access host <IPv6> {log [all|denied-only]}
ipv6 restrict-access host <IPv6> {subnet <IPv6-PREFIX> {log [all|denied-only]}}

ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>

ipv6 restrict-access subnet <IPv6-PREFIX> {host|log}
ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}
ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}

Parameters

- ipv6 restrict-access host <IPv6> {log [all|denied-only]}

<table>
<thead>
<tr>
<th>host &lt;IPv6&gt;</th>
<th>Restricts management access to a specified host, based on the host’s IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
</tbody>
</table>

- ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}

<table>
<thead>
<tr>
<th>host &lt;IPv6&gt;</th>
<th>Restricts management access to a specified host, based on the host’s IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet &lt;IPv6-PREFIX&gt;</td>
<td>Optional. Restricts access to the host on a specified IPv6 subnet</td>
</tr>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
</tbody>
</table>

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

ipv6 restrict-access [host|ipv6-access-list|subnet]

ipv6 restrict-access host <IPv6> {log|subnet}
ipv6 restrict-access host <IPv6> {log [all|denied-only]}
ipv6 restrict-access host <IPv6> {subnet <IPv6-PREFIX> {log [all|denied-only]}}

ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>

ipv6 restrict-access subnet <IPv6-PREFIX> {host|log}
ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}
ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}

Parameters

- ipv6 restrict-access host <IPv6> {log [all|denied-only]}

<table>
<thead>
<tr>
<th>host &lt;IPv6&gt;</th>
<th>Restricts management access to a specified host, based on the host’s IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
</tbody>
</table>

- ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}

<table>
<thead>
<tr>
<th>host &lt;IPv6&gt;</th>
<th>Restricts management access to a specified host, based on the host’s IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet &lt;IPv6-PREFIX&gt;</td>
<td>Optional. Restricts access to the host on a specified IPv6 subnet</td>
</tr>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
</tbody>
</table>
1. `ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>`

   Uses an IPv6 Access Control Lists (ACLs) to filter access requests.
   IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. An existing IPv6 ACL can be created and used in the management policy context to permit or deny access to specific hosts and/or subnets.
   - `<IPv6-ACCESS-LIST-NAME>` – Specify the IPv6 ACL name.

2. `ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}`

   - `subnet <IPv6-PREFIX>` – Restricts management access to a specified IPv6 subnet.
   - `<IPv6-PREFIX>` – Specify the subnet’s IPv6 prefix in the X:X::X:X/M format.
   - `log [all|denied-only]` – Optional. Configures a logging policy for access requests.
     - `all` – Logs all access requests, both denied and permitted.
     - `denied-only` – Logs only denied access events (when a host/subnet is denied access).

3. `ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}`

   - `subnet <IPv6-PREFIX>` – Restricts management access to a specified IPv6 subnet.
   - `<IPv6-PREFIX>` – Specify the subnet’s IPv6 prefix in the X:X::X:X/M format.
   - `host <IPv6>` – Optional. Restricts management access to a specific host within the specified subnet.
   - `<IPv6>` – Specify the host’s IPv6 address.
   - `log [all|denied-only]` – Optional. Configures a logging policy for access requests.
     - `all` – Logs all access requests, both denied and permitted.
     - `denied-only` – Logs only denied access events (when a host/subnet is denied access).

**Examples**

```
rfs7000-37FABE(config-management-policy-test)#ipv6 restrict-access host 2001:fdbc:06cf:0011::13 subnet 2001:fdbc:06cf:0011::0/64 log all
```

```
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  http server
  no ssh
  ipv6 restrict-access host 2001:fdbc:06cf:0011::13 subnet 2001:fdbc:06cf:0011::0/64 log all
rfs7000-37FABE(config-management-policy-test)#
```

**Related Commands**

`no` – Removes management access restriction settings.
Negates a command or reverts values to their default. When used in the config management policy mode, the `no` command negates or reverts management policy settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
no [aaa-login|banner|ftp|http|https|idle-session-timeout|ipv6|privilege-mode-password|restric-access|snmp-server|ssh|t5|telnet|user|service]
no aaa-login tacacs [accounting|authentication|authorization|fallback|policy]
no banner motd
no ftp {password|rootdir}
no [http|https] server
no [idle-session-timeout|privilege-mode-password|restrict-access]
no ipv6 restrict-access
no snmp-server [community|display-vlan-info-per-radio|enable|host|manager|max-pending-requests|request-timeout|suppress-security-configuration-level|throttle|user]
no snmp-server [community <WORD>|display-vlan-info-per-radio|enable traps|host <IP> {<1-65535>]|[manager [all|v1|v2|v3]|max-pending-requests|request-timeout|suppress-security-configuration-level|throttle|user [snmpmanager|snmpoperator|snmptrap]]
no ssh {login-grace-time|port|use-key}
no t5 snmp-server [community|enable|host]
no [telnet|user <USERNAME>]
no service prompt crash-info

**Parameters**
- no <PARAMETERS>

| no <PARAMETERS> | Removes or reverts this Management policy settings based on the parameters passed |
**Examples**

The following example shows the management policy 'test' settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  http server
  https server
  ftp username superuser password 1
  f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
  no ssh
  aaa-login radius external
  aaa-login radius policy test
  idle-session-timeout 100
  banner motd "Have a Good Day"
```

```
rfs7000-37FABE(config-management-policy-test)#no banner motd
rfs7000-37FABE(config-management-policy-test)#no idle-session-timeout
rfs7000-37FABE(config-management-policy-test)#no http server
```

The following example shows the management policy 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  no http server
  https server
  ftp username superuser password 1
  f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
  no ssh
  aaa-login radius external
  aaa-login radius policy test
  idle-session-timeout 0
```

```
rfs7000-37FABE(config-management-policy-test)#
```
15.1.9 privilege-mode-password

```
management-policy
```

Configures the CLI's privilege mode access password

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
privilege-mode-password [1 <PASSWORD>|<PASSWORD>]
```

Parameters

- `privilege-mode-password [1 <PASSWORD>|<PASSWORD>]`

Examples

```
rfs7000-37FABE(config-management-policy-test)#privilege-mode-password testing@1234
rfs7000-37FABE(config-management-policy-test)#show context
    management-policy test
    http server
    no ssh
    privilege-mode-password 1 2e9f038ac2ed27f919ed5a4dce3d30e32f356f2ceff6fbf26a153d0339c734f
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands

```
no
```

Removes the configured CLI privilege mode access password
15.1.10 restrict-access

Restricts management access to a set of hosts or subnets

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access). Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7652, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
restrict-access [host|ip-access-list|subnet]
restrict-access host <IP> {log|subnet}
restrict-access host <IP> {log [all|denied-only]}
restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}
restrict-access ip-access-list <IP-ACCESS-LIST-NAME>
restrict-access subnet <IP/M> {host|log}
restrict-access subnet <IP/M> {log [all|denied-only]}
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

Parameters
- **restrict-access host <IP> {log [all|denied-only]}**
  - host <IP> — Restricts management access to a specified host, based on the host’s IPv4 address
    - <IP> – Specify the host’s IPv4 address.
  - log [all|denied-only] — Optional. Configures a logging policy for access requests
    - all – Logs all access requests, both denied and permitted
    - denied-only – Logs only denied access (when an access request received from a host denied access, a record is logged)

- **restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}**
  - host <IP> — Restricts management access to a specified host, based on the host’s IPv4 address
    - <IP> – Specify the host’s IPv4 address.
  - subnet <IP/M> — Optional. Restricts access to the host on a specified subnet
    - <IP/M> – Specify the subnet’s IPv4 address and mask in the A.B.C.D/M format.
  - log [all|denied-only] — Optional. Configures a logging policy for access requests
    - all – Logs all access requests, both denied and permitted
    - denied-only – Logs only denied access events (when access request received from a host is denied)
### restrict-access ip-access-list <IP-ACCESS-LIST-NAME>

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses an IPv4 ACL to filter access requests. IPv4 ACLs filter/mark packets based on the IPv4 address from which they arrive. IP and non-IP traffic, on the same layer 2 interface, can be filtered by applying an IPv4 ACL. Each IPv4 ACL contains a set of deny and/or permit rules. Each rule is specific to source and destination IPv4 addresses and the unique rules and precedence definitions assigned. When the network traffic matches the criteria specified in one of these rules, the action defined in that rule is used to determine whether the traffic is allowed or denied.</td>
<td><code>restrict-access ip-access-list &lt;IP-ACCESS-LIST-NAME&gt;</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP-ACCESS-LIST-NAME&gt;</code></td>
<td>Specify the IPv4 ACL name.</td>
</tr>
</tbody>
</table>

### restrict-access subnet <IP/M> {log [all|denied-only]}

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricts management access to a specified subnet. IPv4 ACLs filter/mark packets based on the IPv4 address from which they arrive. IP and non-IP traffic, on the same layer 2 interface, can be filtered by applying an IPv4 ACL. Each IPv4 ACL contains a set of deny and/or permit rules. Each rule is specific to source and destination IPv4 addresses and the unique rules and precedence definitions assigned. When the network traffic matches the criteria specified in one of these rules, the action defined in that rule is used to determine whether the traffic is allowed or denied.</td>
<td>`restrict-access subnet &lt;IP/M&gt; {log [all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP/M&gt;</code></td>
<td>Specify the subnet’s IPv4 address and mask in the A.B.C.D/M format.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Log Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Logs all access requests, both denied and permitted</td>
</tr>
<tr>
<td><code>denied-only</code></td>
<td>Logs only denied access events (when access request received from a subnet is denied)</td>
</tr>
</tbody>
</table>

### restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricts management access to a specified subnet. IPv4 ACLs filter/mark packets based on the IPv4 address from which they arrive. IP and non-IP traffic, on the same layer 2 interface, can be filtered by applying an IPv4 ACL. Each IPv4 ACL contains a set of deny and/or permit rules. Each rule is specific to source and destination IPv4 addresses and the unique rules and precedence definitions assigned. When the network traffic matches the criteria specified in one of these rules, the action defined in that rule is used to determine whether the traffic is allowed or denied.</td>
<td>`restrict-access subnet &lt;IP/M&gt; {host &lt;IP&gt; {log [all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Specify the host’s IPv4 address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Log Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Logs all access requests, both denied and permitted</td>
</tr>
<tr>
<td><code>denied-only</code></td>
<td>Logs only denied access events (when access request received from a host within the specified subnet is denied)</td>
</tr>
</tbody>
</table>

### Examples

```
rfs7000-37FABE(config-management-policy-test)#restrict-access host 172.16.10.4 log denied-only
```

```
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  no http server
  https server
  ftp username superuser password 1
  f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
  no ssh
  aaa-login radius external
  aaa-login radius policy test
  idle-session-timeout 0
  restrict-access host 172.16.10.4 log denied-only
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes device access restrictions</td>
</tr>
</tbody>
</table>
15.1.11 snmp-server

Enables the Simple Network Management Protocol (SNMP) engine settings. SNMP is an application layer protocol that facilitates the exchange of management information between the controller and a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the controller’s management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string gathers statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system’s performance and other parameters.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
snmp-server [community|enable|display-vlan-info-per-radio|host|manager|max-pending-requests|request-timeout|suppress-security-configuration-level|throttle|user]

snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw] {ip-snmp-access-list <IP-SNMP-ACL-NAME>}

snmp-server enable traps

snmp-server host <IP> [v1|v2c|v3] {<1-65535>}

snmp-server manager [all|v1|v2|v3]

snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]}

snmp-server [display-vlan-info-per-radio|throttle {<1-100>}|suppress-security-configuration-level [0|1]]

snmp-server user [snmpmanager|snmpoperator|snmptrap] snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth|encrypted]

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 {0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>}

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted auth md5|des auth md5} {0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>}
```

Parameters

- **snmp-server community**: Sets the community string and associated access privileges. Enables SNMP access by configuring community strings that act like passwords. Configure different types of community strings, each string providing a different form of access. Provide either read-only (ro) or read-write (rw) access.
  - 0 <WORD> — Sets a clear text SNMP community string
  - 2 <WORD> — Sets an encrypted SNMP community string
  - <WORD> — Sets the SNMP community string
snmp-server enable traps

After configuring the SNMP community string, assign one of the following accesses:

- ro – Assigns read-only access to the specified SNMP community (allows a remote device to retrieve information)
- rw – Assigns read and write access to the specified SNMP community (allows a remote device to modify settings)

snmp-server host <IP> [v1|v2c|v3] {<1-65535>}

- ro – Assigns read-only access to the specified SNMP community (allows a remote device to retrieve information)
- rw – Assigns read and write access to the specified SNMP community (allows a remote device to modify settings)

ip-snmp-access-list <IP-SNMP-ACL-NAME>

Optional. Associates an IP SNMP access list (should be existing and configured). The IP SNMP ACL sets the SNMP management station’s IP address. SNMP trap information is received at this address.

- snmp-server enable traps

enable traps

Enables trap generation (using the trap receiver configuration defined). This feature is disabled by default. Enabling this feature ensures the dispatch of SNMP notifications to all hosts.

In a managed network, the controller uses SNMP trap receivers to notify faults. SNMP traps are unsolicited notifications triggered by thresholds (or actions) on devices and are therefore an important fault management tool.

A SNMP trap receiver is the destination of SNMP messages (external to the controller). A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc.

SNMP trap notifications exist for most controller operations, but not all are necessary for day-to-day operation.

snmp-server host <IP> [v1|v2c|v3] {<1-65535>}

host <IP>

Configures a host’s IP address. This is the external server resource dedicated to receiving SNMP traps on behalf of the controller.

[v1|v2c|v3]

Configures the SNMP version used to send the traps

- v1 – Uses SNMP version 1. This option is disabled by default.
- v2c – Uses SNMP version 2c. This option is disabled by default.
- v3 – Uses SNMP version 3. This option is enabled by default.

<1-65535>

Optional. Configures the virtual port of the server resource dedicated to receiving SNMP traps

- <1-65535> – Optional. Specify a value from 1 - 65535. The default port is 162.

snmp-server manager [all|v1|v2|v3]

manager [all|v2|v3]

Enables SNMP manager and specifies the SNMP version

- all – Enables SNMP manager version v2 and v3
- v1 – Enables SNMP manager version v1 only. SNMPv1 uses a simple password (“community string”). Data is unencrypted (clear text). Consequently it provides limited security, and should be used only inside LANs behind firewalls, not in WANs.
- v2 – Enables SNMP manager version v2 only. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPv2 is enabled by default.

Contd..
- **v3** – Enables SNMP manager version v3 only. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *User-based Security Model (USM)* for message security and the *View-based Access Control Model (VACM)* for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

- **snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]**

  - **max-pending-requests {<64-1024>}**
    - Sets the maximum number of requests that can be pending at any given time
    - **<64-1024>** – Optional. Specify a value from 64 - 1024. The default is 128.

  - **request-timeout {<2-720>}**
    - Sets the interval, in seconds, after which an error message is returned for a pending request
    - **<2-720>** – Optional. Specify a value from 2 - 720 seconds. The default is 240 seconds.

- **snmp-server [display-vlan-info-per-radio|throttle <1-100>|suppress-security-configuration-level [0|1]]**

  - **display-vlan-info-per-radio**
    - Enables the display of the VLAN ID along with the radio interface ID

  - **throttle <1-100>**
    - Sets CPU usage for SNMP activities. Use this command to set the CPU usage from 1 - 100.

  - **suppress-security-configuration-level [0|1]**
    - Sets the level of suppression of SNMP security configuration information
      - **0** – If this option is selected, an empty string is returned for the SNMP request for security configuration information. Security configuration information consists of:
        - Passwords
        - Keys
        - Shared secrets
      - The default setting is 0.
      - **1** – Suppresses the display of the policy, IP ACL, passwords, keys and shared secrets. If this option is selected, in addition to suppression from ‘Level 0’, an empty string is returned for a SNMP request on following items:
        - Management policies
        - IP ACL
        - Tables containing user names and community strings

- **snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD> | 2 <ENCRYPTED-PASSWORD> | <PASSWORD>]**

  - **user [snmpmanager|snmpoperator|snmptrap]**
    - Defines user access to the SNMP engine
      - snmpmanager – Sets user as a SNMP manager
      - snmpoperator – Sets user as a SNMP operator
      - snmptrap – Sets user as a SNMP trap user

  - **v3 auth md5**
    - Uses SNMP version 3 as the security model
      - **auth** – Uses an authentication protocol
      - **md5** – Uses HMAC-MD5 algorithm for authentication

  - **[0 <PASSWORD> | 2 <ENCRYPTED-PASSWORD> | <PASSWORD>]**
    - Configures password using one of the following options:
      - **0 <PASSWORD>** – Configures clear text password
      - **2 <ENCRYPTED-PASSWORD>** – Configures encrypted password
      - **<PASSWORD>** – Specifies a password for authentication and privacy protocols
### snmp-server user \[snmpmanager|snmpoperator|snmptrap\] v3 encrypted

| user \[snmpmanager|snmpoperator|snmptrap\] | Defines user access to the SNMP engine |
|------------------------------------------|----------------------------------------|
|                                         | • snmpmanager – Sets user as a SNMP manager |
|                                         | • snmpoperator – Sets user as a SNMP operator |
|                                         | • snmptrap – Sets user as a SNMP trap user |
| v3 encrypted | Uses SNMP version 3 as the security model |
|             | • encrypted – Uses encrypted privacy protocol |
| auth md5 | Uses authentication protocol |
|           | • auth – Sets authentication parameters |
|           | • md5 – Uses HMAC-MD5 algorithm for authentication |
| des auth md5 | Uses privacy protocol for user privacy |
|             | • des – Uses CBC-DES for privacy |
|             | After specifying the privacy protocol, specify the authentication mode. |
|             | • auth – Sets user authentication parameters |
|             | • md5 – Uses HMAC-MD5 algorithm for authentication |

| [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>] | The following are common to both the auth and des parameters: |
|-------------------------------------------------|------------------------------------------------|
|                                                  | Configures password using one of the following options: |
|                                                  | • 0 <PASSWORD> – Configures a clear text password |
|                                                  | • 2 <ENCRYPTED-PASSWORD> – Configures an encrypted password |
|                                                  | • <PASSWORD> – Specifies a password for authentication and privacy protocols |

### Examples

```
rfs7000-37FABE(config-management-policy-test)#snmp-server community snmp1 ro
rfs7000-37FABE(config-management-policy-test)#snmp-server host 172.16.10.23 v3 162
rfs7000-37FABE(config-management-policy-test)#commit
rfs7000-37FABE(config-management-policy-test)#snmp-server user snmpmanager v3 auth md5 test@123
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  no http server
  https server
  ftp username superuser password 1
  f617ca50c59f047028f96db4baab8f3d8f03c03abc257960b0fd127c69f02cd7e rootdir dir
  no ssh
  snmp-server community snmp1 ro
  snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
  snmp-server host 172.16.10.23 v3 162
  aaa-login radius external
  aaa-login radius policy test
  idle-session-timeout 0
  restrict-access host 172.16.10.2 log all
```

### Related Commands

| no | Disables or resets the SNMP server settings |
### 15.1.12 ssh

**management-policy**

Enables Secure Shell (SSH) for this management policy

SSH, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ssh {login-grace-time <60-300>|port <1-65535>}

**Parameters**
- ssh {login-grace-time <60-300>|port <1-65535>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td>Enables SSH communication between client and server</td>
</tr>
<tr>
<td>login-grace-time</td>
<td>Optional. Configures the login grace time. This is the interval, in seconds, after which an unsuccessful login is disconnected.</td>
</tr>
<tr>
<td>&lt;60-300&gt;</td>
<td>• &lt;60-300&gt; – Specify a value from 60 - 300 seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Configures the SSH port. This is the port used for SSH connections.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>• &lt;1-65535&gt; – Specify a value from 1 - 165535. The default port is 22.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-management-policy-test)#ssh port 162

rfs7000-37FABE(config-management-policy-test)#show context

management-policy test

no http server

https server

ftp username superuser password 1

f617ca50c59f4b47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir

ssh port 162

snmp-server community snmpl ro

snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123

snmp-server host 172.16.10.23 v3 162

aaa-login radius external

aaa-login radius policy test

idle-session-timeout 0

restrict-access host 172.16.10.2 log all

rfs7000-37FABE(config-management-policy-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets SSH access port to factory default (port 22)</td>
</tr>
</tbody>
</table>
15.1.13 t5

\*management-policy

Configures SNMP server settings for T5 devices on this management policy.

A T5 controller is an external device that can be adopted and managed by a WiNG controller. When enabled as a supported external device, a T5 controller can provide data to WiNG to assist in its management within a WiNG supported subnet.

This command enables SNMP to communicate with T5 devices within the network. SNMP facilitates the exchange of management information between the controller or service platform and the T5 device. For more information, see `snmp-server`.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
t5 snmp-server [community|contact|enable|host|location]
```

```
t5 snmp-server community <COMMUNITY-NAME> [ro|rw] <SNMP-STATION-IP>
```

```
t5 snmp-server contact <LINE>
```

```
t5 snmp-server enable [server|traps]
```

```
t5 snmp-server host <IP>
```

```
t5 snmp-server location <LINE>
```

**Parameters**

- **t5 snmp-server community <COMMUNITY-NAME> [ro|rw] <SNMP-STATION-IP>**

  - **community <COMMUNITY-NAME> [ro|rw]**
    - Defines a public or private community designation. By default, SNMPv2 community strings on most devices are set to public, for the read-only community string, and private for the read-write community string.
    - `<COMMUNITY-NAME>` – Specify the SNMP community name, and configure the access permission for this community string (used by devices to retrieve or modify information).
    - `ro` – Allows a remote device to retrieve information only
    - `rw` – Allows a remote device to retrieve information and modify settings

  - `<SNMP-STATION-IP>`
    - Specify the SNMP management station IP address for receiving trap information

- **t5 snmp-server contact <LINE>**

  - **contact <LINE>**
    - Configures the administrator of SNMP trap events for the T5 controller.
    - `<LINE>` – Specify the administrator’s name (should not exceed 64 characters).

- **t5 snmp-server enable [server|traps]**

  - **enable [server|traps]**
    - Enables the following:
      - `server` – Enables the SNMP server. When enabled, the system accepts SNMP management data. This is enabled by default.
      - `traps` – Enables SNMP traps. When enabled, the system generates SNMP traps. This is enabled by default.
### t5 snmp-server host <IP>

| host <IP> | Configures the T5 SNMP host's IP address. The SNMP host receives the SNMP notifications.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;IP&gt; – Specify the SNMP host's IP address.</td>
</tr>
</tbody>
</table>

### t5 snmp-server location <LINE>

<table>
<thead>
<tr>
<th>location &lt;LINE&gt;</th>
<th>Configures the system location for SNMP traps.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LINE&gt; – Specify the SNMP trap location (should not exceed 64 characters).</td>
</tr>
</tbody>
</table>

#### Examples

```
 nx9500-6C8809(config-management-policy-test)#t5 snmp-server community lab rw 192.168.13.7
```

```
x9500-6C8809(config-management-policy-test)#show context
management-policy test
  http server
  no ssh
  t5 snmp-server community lab rw 192.168.13.7
```

#### Related Commands

<table>
<thead>
<tr>
<th>no</th>
<th>Removes or reverts SNMP server configuration for T5 devices</th>
</tr>
</thead>
</table>

15.1.14 telnet

Enabled Telnet. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.

By default Telnet, when enabled, uses Transmission Control Protocol (TCP) port 23. Use this command to change the TCP port.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

telnet {port <1-65535>}

Parameters

- `telnet {port <1-65535>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>telnet</td>
<td>Enables Telnet</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Configures the Telnet port. This is the port used for Telnet connections.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;1-65535&gt;</code> – Sets a value from 1 - 65535. The default port is 23.</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-management-policy-test)#telnet port 200

rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
  telnet port 200
  no http server
  https server
  ftp username superuser password 1
  f617ca50c59fb47028f96db4baab8f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
  ssh port 162
  snmp-server community smipl ro
  snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
  snmp-server host 172.16.10.23 v3 162
  aaa-login radius external
  aaa-login radius policy test
  idle-session-timeout 0
  restrict-access host 172.16.10.2 log all
  rfs7000-37FABE(config-management-policy-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables Telnet</td>
</tr>
</tbody>
</table>
### 15.1.15 user

- **management-policy**
  - Adds new user account

**Supported in the following platforms:**
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>]
role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|web-user-admin] access [all|console|ssh|telnet|web]
(allowed-locations <ALLOWED-LOCATIONS>)
```

**Parameters**

- **user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role [device-
provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-
admin|web-user-admin] access [all|console|ssh|telnet|web]
(allowed-locations <ALLOWED-LOCATIONS>)

<table>
<thead>
<tr>
<th>user &lt;USERNAME&gt;</th>
<th>Adds new user account to this management policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;USERNAME&gt; – Sets the username</td>
</tr>
</tbody>
</table>

| password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] | Configures a password |
|-------------------|-------------------------------------------------|
|                   | • 0 <PASSWORD> – Sets a clear text password    |
|                   | • 1 <SHA1-PASSWORD> – Sets the SHA1 hash of the password |
|                   | • <PASSWORD> – Sets the password               |

<table>
<thead>
<tr>
<th>role</th>
<th>Configures the user role. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• device-provisioning-admin – Device provisioning administrator. Has privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a devices existing configuration unless the configuration is properly archived.</td>
</tr>
<tr>
<td></td>
<td>• helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as clear statistics, reboot, create and copy technical support dumps. The helpdesk administrator can also create a guest user account and password for registration. These details can be e-mailed or sent as SMS to mobile phone.</td>
</tr>
<tr>
<td></td>
<td>• monitor – Monitor. Has read-only access to the system. Can view configuration and statistics except for secret information</td>
</tr>
<tr>
<td></td>
<td>• network-admin – Network administrator. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF</td>
</tr>
<tr>
<td></td>
<td>• security-admin – Security administrator. Modifies WLAN keys and passphrases</td>
</tr>
<tr>
<td></td>
<td>• superuser – Superuser. Has full access, including halt and delete startup-config</td>
</tr>
<tr>
<td></td>
<td>• system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access</td>
</tr>
<tr>
<td></td>
<td>• web-user-admin – Web user administrator. This role is used to create guest users and credentials. The Web user admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.</td>
</tr>
</tbody>
</table>
### Examples

```
rfs7000-37FABE(config-management-policy-test)#user TESTER password test123 role superuser access all
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
telnet port 200
no http server
https server
ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
ssh port 162
user TESTER password 1 b6b37c51405f4e93c67fe8af82d450c9fd6af69324cd56a55055cefe695b6a14
role superuser access all
snmp-server community snmp1 ro
snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
snmp-server host 172.16.10.23 v3 162
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 0
restrict-access host 172.16.10.2 log all
rfs7000-37FABE(config-management-policy-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a user account</td>
</tr>
</tbody>
</table>
15.1.16 service

Invokes service commands

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

service [prompt|show]
service [prompt crash-info|show cli]

Parameters

- service [prompt crash-info|show cli]

<table>
<thead>
<tr>
<th>service prompt crash-info</th>
<th>Updates CLI prompt settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• crash-info – Includes an asterix at the end of the prompt if the device has crash files in the flash:/crashinfo folder</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>service show cli</th>
<th>Displays running system information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• cli – Displays the current mode’s CLI tree</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-management-policy-test)#service show cli
Management Mode mode:
++-help [help]
  ++-search
    ++-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
    ++-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
    ++-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
    ++-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
    ++-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
  ++-show
    ++-commands [show commands]
    ++-simulate
    ++-stats [show simulate stats]
    ++-eval
    ++-WORD [show eval WORD]
  ++-debugging [show debugging (|{on DEVICE-OR-DOMAIN-NAME})]
    ++-cfgd [show debugging cfgd]
    ++-on
      ++-DEVICE-OR-DOMAIN-NAME [show debugging (|{on DEVICE-OR-DOMAIN-NAME})]
      ++-fib [show debugging fib(|{on DEVICE-NAME})]
      ++-on
        ++-DEVICE-NAME [show debugging fib(|{on DEVICE-NAME})]
    ++-wireless [show debugging wireless (|{on DEVICE-OR-DOMAIN-NAME})]
    ++-on
--More--

Related Commands

| no | Disables the inclusion of an asterix indicator notifying the presence of crash files |
CHAPTER 16
RADIUS-POLICY

This chapter summarizes the RADIUS group, server, and user policy commands in the CLI command structure. Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to authenticate users and authorize their access to the network. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the local RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to a network, the authentication request is sent to the local RADIUS server. The authentication and encryption of communications takes place through the use of a shared secret password (not transmitted over the network).

The local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assigns policies for group authorization.

Controllers and access points allow enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. A certificate is required for EAP TTLS, PEAP, and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after RADIUS server authentication. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

The chapter is organized into the following sections:

- `radius-group`
- `radius-server-policy`
- `radius-user-pool-policy`

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
16.1 radius-group

This section describes RADIUS user group configuration commands. The local RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the local database. The user ID in the received access request is mapped to the associated wireless group for authentication. The configuration of groups allows enforcement of the following policies that control user access:

- Assign a VLAN to the user upon successful authentication
- Define start and end of time (HH:MM) when the user is allowed to authenticate
- Define the SSID list to which a user, belonging to this group, is allowed to associate
- Define the days of the week the user is allowed to login
- Rate limit traffic (for non-management users)

RADIUS users are categorized into three groups: normal user, management user, and guest user. A RADIUS group not configured as management or guest is a normal user group. User access and role settings depends on the RADIUS group the user belongs.

Use the (config) instance to configure RADIUS group commands. This command creates a group within the existing RADIUS group. To navigate to the RADIUS group instance, use the following commands:

```plaintext
<DEVICE>(config)#radius-group <GROUP-NAME>
```

```plaintext
rfs7000-37FABE(config)#radius-group test
rfs7000-37FABE(config-radius-group-test)#?
```

Radius user group configuration commands:
- guest: Make this group a Guest group
- no: Negate a command or set its defaults
- policy: Radius group access policy configuration
- rate-limit: Set rate limit for group
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

```plaintext
rfs7000-37FABE(config-radius-group-test)#
```

### NOTE:
The RADIUS group name cannot exceed 32 characters, and cannot be modified as part of the group edit process.
The following table summarizes RADIUS group configuration commands:

**Table 16.1** RADIUS-Group-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest</td>
<td>Enables guest access for the newly created group</td>
<td>page 16-4</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 16-10</td>
</tr>
<tr>
<td>policy</td>
<td>Configures RADIUS group access policy parameters</td>
<td>page 16-5</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Sets the default rate limit per user in Kbps, and applies it to all enabled WLANs</td>
<td>page 16-9</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *Chapter 5, COMMON COMMANDS.*
16.1.1 guest

*radius-group*

Configures this group as a guest (non-management) group. A guest user group has temporary permissions to the controller’s local RADIUS server. You can configure multiple guest user groups, each having a unique set of settings. Guest user groups cannot be made management groups with access and role permissions.

Guest users and policies are used for captive portal authorization to the network.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

guest

**Parameters**

None

**Examples**

```bash
rfs7000-37FABE(config-radius-group-test)#guest
rfs7000-37FABE(config-radius-group-test)#show context radius-group test guest
rfs7000-37FABE(config-radius-group-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Makes this group a non-guest group</td>
</tr>
</tbody>
</table>
16.1.2 policy

 Sets a RADIUS group’s authorization settings, such as access day/time, WLANs etc.

 **NOTE:** A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN.

 Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

 **Syntax**

 policy [access|day|inactivity-timeout|role|ssid|time|vlan]

 policy vlan <1-4094>

 policy access [all|console|ssh|telnet|web] { (all|console|ssh|telnet|web) }

 policy day [all|fr|mo|sa|su|th|tu|we|weekdays] { (fr|mo|sa|su|th|tu|we|weekdays) }

 policy inactivity-timeout <60-86400>

 policy role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]

 policy ssid <SSID>

 policy time start <HH:MM> end <HH:MM>

 **NOTE:** Access and role settings are applicable only to a management group. They cannot be configured for a RADIUS non-management group.

 **Parameters**

- **policy vlan <1-4094>**

  vlan <1-4094> Sets the guest RADIUS group’s VLAN ID from 1 - 4094. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server).

  **Note:** This option applicable to a guest user group, which has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each group. Guest user groups cannot be made management groups with unique access and role permissions.

  **Note:** Enable dynamic VLAN assignment for the WLAN for the VLAN assignment to take effect.
• policy access [all|console|ssh|telnet|web] { (all|console|ssh|telnet|web) }

access

Configures access type for a management group. Management groups can be assigned unique access and role permissions.

• all – Allows all access. Wireless client access to the console, ssh, telnet, and/or Web
• console – Allows console access only
• ssh – Allows SSH access only
• telnet – Allows Telnet access only
• web – Allows Web access only

These parameters are recursive, and you can provide access to more than one component.

• policy role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]

role

Configures the role assigned to a management RADIUS group. If a group is listed as a management group, it may also have a unique role assigned. Available roles include:

• device-provisioning-admin – Device provisioning administrator. Has privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a device's existing configuration unless the configuration is properly archived.
• helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as clear statistics, reboot, create and copy tech support dumps. The helpdesk administrator can also create a guest user account and password for registration. These details can be e-mailed or sent as SMS to a mobile phone.
• monitor – Monitor. Has read-only access to the network. Can view configuration and statistics except for secret information
• network-admin – Network administrator. Has wired and wireless access to the network. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF
• security-admin – Security administrator. Has full read/write access to the network. Modifies WLAN keys and passphrases
• superuser – Superuser. Has full access, including halt and delete startup config
• system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access
• web-user-admin – Web user administrator. This role is used to create guest users and credentials. The web-user-admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.

• policy inactivity-timeout <60-86400>

inactivity-timeout

Configures the inactivity time for this RADIUS group users. If a frame is not received from a client for the specified period, then the client’s session is removed. When defined, this value is used instead of the captive-portal inactivity timeout. If the inactivity timeout is not configured in the radius-group context or the captive-portal context, the default timeout (60 seconds) is applied.

• <60-86400> – Specify a value from 60 - 86400 seconds.
## RADIUS-POLICY 16-7

### Usage Guidelines

A management group access policy provides:

- access details
- user roles
- policy’s start and end time

The SSID, day, and VLAN settings are not applicable to a management user group.

### Examples

The following example shows a RADIUS guest group settings:

```
rfs7000-37FABE(config-radius-group-test)#policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#policy day all
rfs7000-37FABE(config-radius-group-test)#policy vlan 1
rfs7000-37FABE(config-radius-group-test)#policy ssid test
```
rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
  guest
  policy vlan 1
  policy ssid test
  policy day mo
  policy day tu
  policy day we
  policy day th
  policy day fr
  policy day sa
  policy day su
  policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#

The following example shows a RADIUS management group settings:

rfs7000-37FABE(config-radius-group-management)#policy access console ssh telnet
rfs7000-37FABE(config-radius-group-management)#policy role network-admin
rfs7000-37FABE(config-radius-group-management)#policy time start 9:30 end 20:30

rfs7000-37FABE(config-radius-group-management)#show context
radius-group management
  policy time start 9:30 end 20:30
  policy access console ssh telnet web
  policy role network-admin
rfs7000-37FABE(config-radius-group-management)#

Related Commands

| no | Removes or modifies a RADIUS group's access settings |
### 16.1.3 rate-limit

 Sets the rate limit for the guest RADIUS server group

 Supported in the following platforms:

 - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
 - Wireless Controllers — RFS4000, RFS6000, RFS7000
 - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

 **Syntax**

```bash
rate-limit [from-air|to-air] <100-1000000>
```

**Parameters**

- `rate-limit [from-air|to-air] <100-1000000>`

  - **to-air <100-1000000>**
    - Sets the rate limit in the downlink direction, from the network to the wireless client
    - `<100-1000000>` — Specify the rate from 100 - 1000000 Kbps.

  - **from-air <100-1000000>**
    - Sets the rate limit in the uplink direction, from the wireless client to the network
    - `<100-1000000>` — Specify the rate from 100 - 1000000 Kbps.

**Examples**

```bash
rfs7000-37FABE(config-radius-group-test)#rate-limit to-air 200
rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
guest
  policy vlan 1
  policy ssid test
  policy day mo
  policy day tu
  policy day we
  policy day th
  policy day fr
  policy day sa
  policy day su
  rate-limit to-air 200
  policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#
```

**Related Commands**

- `no`
  - Removes the RADIUS guest group's rate limits
16.1.4 no

Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the `no` command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
no [guest|policy|rate-limit]
```

```
no policy [access|day|inactivity-timeout|role|ssid|time|vlan]
```

```
no policy access [all|console|ssh|telnet|web]
no policy day [all|fr|mo|sa|su|th|tu|we|weekdays]
no policy ssid [<SSID>|all]
no policy [inactivity-timeout|role|time|vlan]
```

```
no rate-limit [from-air|to-air]
```

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the `no` command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID. |

Examples

The following example shows the RADIUS guest group ‘test’ settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-radius-group-test)#show context radius-group test
   guest
   policy vlan 1
   policy ssid test
   policy day mo
   policy day tu
   policy day we
   policy day th
   policy day fr
   policy day sa
   policy day su
   rate-limit to-air 200
   policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#
```

```
rfs7000-37FABE(config-radius-group-test)#no guest
rfs7000-37FABE(config-radius-group-test)#no rate-limit to-air
rfs7000-37FABE(config-radius-group-test)#no policy day all
```
The following example shows the RADIUS guest group 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
  policy vlan 1
  policy ssid test
  policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#
```
16.2 radius-server-policy

**RADIUS-POLICY**

Creates an onboard device RADIUS server policy and enters its configuration mode.

A RADIUS server policy is a unique authentication and authorization configuration that receives user connection requests, authenticates users, and returns configuration information necessary for the RADIUS client to deliver service to the user. The client is the entity with authentication information requiring validation. The local RADIUS server has access to a database of authentication information used to validate the client's authentication request.

The local RADIUS server uses authentication schemes like PAP, CHAP, or EAP to verify and confirm information provided by a user. The user's proof of identification is verified, along with, optionally, other information. A local RADIUS server policy can also be configured to refer to an external Lightweight Directory Access Protocol (LDAP) resource to verify a user's credentials.

Use the (config) instance to configure RADIUS-Server-Policy related parameters. To navigate to the RADIUS-Server-Policy instance, use the following commands:

```
<DEVICE>(config)#radius-server-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#radius-server-policy test
rfs7000-37FABE(config-radius-server-policy-test)#?
```

Radius Configuration commands:

- **authentication**: Configures RADIUS authentication settings
- **bypass**: Bypass Certificate Revocation List (CRL) check
- **chase-referral**: Enable LDAP server referral chasing
- **crl-check**: Enable Certificate Revocation List (CRL) check
- **ldap-agent**: LDAP Agent configuration parameters
- **ldap-group-verification**: Enable LDAP Group Verification setting
- **ldap-server**: LDAP server parameters
- **local**: RADIUS local realm
- **nas**: RADIUS client
- **no**: Negate a command or set its defaults
- **proxy**: RADIUS proxy server
- **session-resumption**: Enable session resumption/fast reauthentication by using cached attributes
- **termination**: Enable Eap termination for proxy requests
- **use**: Set setting to use
- **clrscr**: Clears the display screen
- **commit**: Commit all changes made in this session
- **do**: Run commands from Exec mode
- **end**: End current mode and change to EXEC mode
- **exit**: End current mode and down to previous mode
- **help**: Description of the interactive help system
- **revert**: Revert changes
- **service**: Service Commands
- **show**: Show running system information
- **write**: Write running configuration to memory or terminal

```
rfs7000-37FABE(config-radius-server-policy-test)#
```

The following table summarizes RADIUS server policy configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Configures RADIUS authentication settings</td>
<td>page 16-14</td>
</tr>
<tr>
<td>bypass</td>
<td>Enables bypassing of CRL check</td>
<td>page 16-16</td>
</tr>
<tr>
<td>chase-referral</td>
<td>Enables LDAP server referral chasing</td>
<td>page 16-17</td>
</tr>
<tr>
<td>crl-check</td>
<td>Enables a certificate revocation list (CRL) check</td>
<td>page 16-18</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>ldap-agent</td>
<td>Configures the LDAP agent's settings</td>
<td>page 16-19</td>
</tr>
<tr>
<td>ldap-group-verification</td>
<td>Enables LDAP group verification</td>
<td>page 16-21</td>
</tr>
<tr>
<td>ldap-server</td>
<td>Configures the LDAP server's settings</td>
<td>page 16-22</td>
</tr>
<tr>
<td>local</td>
<td>Configures a local RADIUS realm</td>
<td>page 16-25</td>
</tr>
<tr>
<td>nas</td>
<td>Configures the key sent to a RADIUS client</td>
<td>page 16-26</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets the RADIUS server policy's settings</td>
<td>page 16-27</td>
</tr>
<tr>
<td>proxy</td>
<td>Configures the RADIUS proxy server's settings</td>
<td>page 16-29</td>
</tr>
<tr>
<td>session-resumption</td>
<td>Enables session resumption</td>
<td>page 16-31</td>
</tr>
<tr>
<td>termination</td>
<td>Enables EAP termination on this current RADIUS server policy. When enabled, EAP authentication is terminated at the controller level.</td>
<td>page 16-32</td>
</tr>
<tr>
<td>use</td>
<td>Defines settings used with the RADIUS server policy</td>
<td>page 16-33</td>
</tr>
</tbody>
</table>
### 16.2.1 authentication

**radius-server-policy**

Specifies the RADIUS datasource used for user authentication. Options include local for the local user database or LDAP for a remote LDAP resource.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
authentication [data-source|eap-auth-type]
```

```
authentication data-source [ldap|local]
```

```
authentication data-source [ldap {fallback}|local] {(ssid <SSID> precedence <1-5000>)}
```

```
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]
```

**Parameters**

- **authentication data-source [ldap {fallback}|local] {(ssid <SSID> precedence <1-5000>)}**

| data-source      | The RADIUS server can either use the local database or an external LDAP server to authenticate a user. It is necessary to specify the data source. The options are: LDAP and local.  
|------------------|---|
| **Note:** The default setting is local.  
| **ldap fallback** | Uses a remote LDAP server as the data source  
| fallback – Optional. Enables fallback to local authentication. This feature ensures that when the configured LDAP data source is unreachable, the client is authenticated against the local RADIUS resource. This option is disabled by default.  
| **local** | Uses the local user database to authenticate a user  
| **ssid <SSID> precedence <1-5000>** | The following keywords are recursive and common to both 'ldap' and 'local' parameters:  
| ssid – Optional. Associates the data source, selected in the previous step, with a SSID  
| <SSID> – Specify the SSID for this authentication data source. The SSID is case sensitive and should not exceed 32 characters in length. Do not use any of the following characters (< > | " & \ ? ,).  
| precedence <SSID> – Sets the precedence for this authentication rule. The precedence value allows systematic evaluation and application of rules. Rules with the lowest precedence receive the highest priority.  
| <1-5000> – Specify a precedence from 1-5000.  
| **Note:** Specifying the SSID allows the RADIUS server to use the SSID attribute in access requests to determine the data source to use. This option is applicable to onboard RADIUS servers only.  

---
- authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]

<table>
<thead>
<tr>
<th>eap-auth-type</th>
<th>Uses Extensible Authentication Protocol (EAP), with this RADIUS server policy, for user authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables both TTLS and PEAP authentication. This is the default setting.</td>
</tr>
<tr>
<td>peap-gtc</td>
<td>Enables PEAP with default authentication using GTC</td>
</tr>
<tr>
<td>peap-mschapv2</td>
<td>Enables PEAP with default authentication using MSCHAPv2</td>
</tr>
<tr>
<td>tls</td>
<td>Enables TLS as the EAP type</td>
</tr>
<tr>
<td>ttls-md5</td>
<td>Enables TTLS with default authentication using md5</td>
</tr>
<tr>
<td>ttls-mschapv2</td>
<td>Enables TTLS with default authentication using MSCHAPv2</td>
</tr>
<tr>
<td>ttls-pap</td>
<td>Enables TTLS with default authentication using PAP</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-radius-server-policy-test)#authentication eap-auth-type tls

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
  authentication eap-auth-type tls
rfs7000-37FABE(config-radius-server-policy-test)#

Related Commands

- no | Removes the RADIUS authentication settings
16.2.2 bypass

radius-server-policy

Enables bypassing a CRL check. When enabled, this feature bypasses checks for missing and expired CRLs. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
bypass [crl-check|expired-crl]

Parameters
- bypass [crl-check|expired-crl]

Bypasses CRL check based on the parameters passed
- crl-check – Bypasses CRL check of missing CRLs
- expired-crl – Bypasses CRL check of expired CRLs

Note: A CRL is a list of certificates that have been revoked or are no longer valid.

Examples
nx9500-6C8809(config-radius-server-policy-test)#bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)#no bypass crl-check

nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
   no bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)#

Related Commands

- no
  Disables bypassing of checking for missing CRLs or expired CRLs
16.2.3 chase-referral

Enables chasing of referrals from an external LDAP server resource

An LDAP referral is a controller or service platform's way of indicating to a client it does not hold the section of the directory tree where a requested content object resides. The referral is the controller or service platform’s direction to the client a different location is more likely to hold the object, which the client uses as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the domain controller to generate another referral, although it usually does not take long to discover the object does not exist and inform the client.

This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

chase-referral

Parameters

None

Examples

rfs7000-37FABE(config-radius-server-policy-test)#chase-referral

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables LDAP server referral chasing</td>
</tr>
</tbody>
</table>
16.2.4 **crl-check**

- **radius-server-policy**

Enables a *certificate revocation list* (CRL) check on this RADIUS server policy. A CRL is a list of revoked certificates issued and subsequently revoked by a *Certification Authority* (CA). Certificates can be revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. The mechanism used for certificate revocation depends on the CA. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
crl-check

**Parameters**

None

**Examples**

rfs7000-37FABE(config-radius-server-policy-test)#crl-check

rfs7000-37FABE(config-radius-server-policy-test)#show context radius-server-policy test
  authentication eap-auth-type tls
crl-check
rfs7000-37FABE(config-radius-server-policy-test)#

**Related Commands**

| **no** | Enables CRL check on a RADIUS server policy |
### 16.2.5 ldap-agent

#### radius-server-policy

Configures the LDAP agent’s settings in the RADIUS server policy context.

When a user’s credentials are stored on an external LDAP server, the local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource (using credentials maintained locally).

This feature is available to all controller, service platforms and access point models, with the exception of AP6511 and AP6521 models running in standalone AP or virtual controller AP mode. However, this feature is supported by dependent mode AP6511 and AP6521 model access points when adopted and managed by a controller or service platform.

Supported in the following platforms:
- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ldap-agent [join|join-retry-timeout|primary|secondary]
ldap-agent [join {on <DEVICE-NAME>}]|join-retry-timeout <60-300>]
ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME> domain-admin-user <ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

**Parameters**

- **ldap-agent [join {on <DEVICE-NAME>}]|join-retry-timeout <60-300>]**

<table>
<thead>
<tr>
<th>ldap-agent</th>
<th>Configures the LDAP agent’s settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>join {on &lt;DEVICE-NAME&gt;}</td>
<td>Initiates the join process, which binds the RADIUS server with the LDAP server’s (Windows) domain. When successful, the hostname (name of the AP, wireless controller, or service platform) is added to the LDAP server’s Active Directory.</td>
</tr>
<tr>
<td>join-retry-timeout &lt;60-300&gt;</td>
<td>If the join process fails (i.e. the RADIUS server fails to join the LADP server’s domain), the process is retried after a specified interval. This command configures the interval (in seconds) between two successive join attempts.</td>
</tr>
</tbody>
</table>

**Note:** To confirm the join status of a controller, use the `show > ldap-agent > join-status` command.

**join-retry-timeout <60-300>**
- Set the timeout value from 60 - 300 seconds. The default is 60 seconds.

**Note:** A retry timer is initiated as soon as the join process starts, which tracks the time lapse in case of a failure.
• ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME> domain-admin-user <ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-agent</td>
<td>Configures the LDAP agent’s settings</td>
</tr>
<tr>
<td>primary</td>
<td>Configures the primary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the primary LDAP server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the secondary LDAP server.</td>
</tr>
<tr>
<td>domain-name &lt;LDAP-DOMAIN-NAME&gt;</td>
<td>This keyword is common to both the ‘primary’ and ‘secondary’ parameters.</td>
</tr>
<tr>
<td></td>
<td>• domain-name – Configures the primary or secondary LDAP server’s domain name</td>
</tr>
<tr>
<td></td>
<td>• &lt;LDAP-DOMAIN-NAME&gt; – Specify the domain name.</td>
</tr>
<tr>
<td>domain-admin-user &lt;ADMIN-USER-NAME&gt;</td>
<td>This keyword is common to both the ‘primary’ and ‘secondary’ parameters.</td>
</tr>
<tr>
<td></td>
<td>• domain-admin-user – Configures the primary or secondary LDAP server’s admin user name</td>
</tr>
<tr>
<td></td>
<td>• &lt;ADMIN-USER-NAME&gt; – Specify the admin user’s name.</td>
</tr>
<tr>
<td>domain-admin-password [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]</td>
</tr>
<tr>
<td></td>
<td>• domain-admin-password – Configures the primary or secondary LDAP server’s admin user password</td>
</tr>
<tr>
<td></td>
<td>• 0 &lt;WORD&gt; – Specifies the password in the unencrypted format</td>
</tr>
<tr>
<td></td>
<td>• 2 &lt;WORD&gt; – Specifies the password in the encrypted format</td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58(config-radius-server-policy-test)#ldap-agent primary domain-name test domain-admin-user Administrator domain-admin-password 0 test@123
rfs4000-229D58(config-radius-server-policy-test)#

rfs4000-229D58(config-radius-server-policy-test)#show context radius-server-policy test
ldap-agent primary domain-name test domain-admin-user Administrator domain-admin-password 0 test@123
rfs4000-229D58(config-radius-server-policy-test)#

Related Commands

no | Removes LDAP agent settings from this RADIUS server policy
16.2.6 *ldap-group-verification*

> radius-server-policy

Enables LDAP group verification settings on this RADIUS server policy. This option is enabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ldap-group-verification

**Parameters**

None

**Examples**

rfs7000-37FABE(config-radius-server-policy-test)#ldap-group-verification
rfs7000-37FABE(config-radius-server-policy-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables LDAP group verification settings</td>
</tr>
</tbody>
</table>
16.2.7 ldap-server

`radius-server-policy`

Configures the LDAP server's settings. Configuring LDAP server allows users to login and authenticate from anywhere on the network.

Administrators have the option of using the local RADIUS server to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative user management overhead making RADIUS authorization more secure and efficient.

RADIUS is not just a database. It is a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the local RADIUS server to free up resources and manage user credentials from a secure remote location. It is the local RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. A LDAP user database alone cannot perform such complex authorization checks.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ldap-server [dead-period|primary|secondary]
```

```
ldap-server dead-period <0-600>
```

```
ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME>
bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD> | 2 <ENCRYPTED-PASSWORD> | <PASSWORD>]
<ATTR> group-attr <ATTR> group-filter <FILTER> group-membership <WORD> {net-timeout <1-10> | start-tls net-timeout <1-10> |
tls-mode net-timeout <1-10>}
```

Parameters

- `ldap-server dead-period <0-600>`

  dead-period <0-600>  Set an interval, in seconds, during which the local server will not contact its LDAP server resource once its been defined as unavailable. A dead period is only implemented when additional LDAP servers are configured and available.
  - <0-600> – Specify a value from 0 - 600 seconds. The default is 300 seconds.

- `ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME> bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD> | 2 <ENCRYPTED-PASSWORD> | <PASSWORD>]
<ATTR> group-attr <ATTR> group-filter <FILTER> group-membership <WORD> {net-timeout <1-10> | start-tls net-timeout <1-10> |
tls-mode net-timeout <1-10>}
```

```
ldap primary Configures the primary LDAP server settings
```

```
ldap secondary Configures the secondary LDAP server settings
```

```
host <IP> Specifies the LDAP host’s IP address
  - <IP> – Specify the LDAP server’s IP address.
```

```
port <1-65535> Configures the LDAP server port
  - <1-65535> – Specify a port between 1 - 65535.
```

```
login <LOGIN-NAME> Configures the login name of a user to access the LDAP server
  - <LOGIN-NAME> – Specify a login ID (should not exceed 127 characters).
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| bind-dn <BIND-DN> | Configures a distinguished bind name. This is the *distinguished name* (DN) used to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas.  
  - `<BIND-DN>` – Specify a bind name (should not exceed 127 characters). |
| base-dn <BASE-DN> | Configures a distinguished base name. This is the DN that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with a specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the *Relative Distinguished Name* (RDN). It identifies an entry distinctly from any other entries that have the same parent  
  - `<BASE-DN>` – Specify a base name (should not exceed 127 characters). |
| passwd [0 | Sets a valid password for the LDAP server.  
  - 0 `<PASSWORD>` – Sets an UNENCRYPTED password  
  - 2 `<ENCRYPTED-PASSWORD>` – Sets an ENCRYPTED password  
  - `<PASSWORD>` – Sets the LDAP server bind password, specified UNENCRYPTED, with a maximum size of 31 characters |
| passwd-attr <ATTR> | Specify the LDAP server password attribute (should not exceed 63 characters). |
| group-attr <ATTR> | Specify a name to configure group attributes (should not exceed 31 characters). LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name. |
| group-filter <FILTER> | Specify a name for the group filter attribute (should not exceed 255 characters). This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service. |
| group-membership <WORD> | Specify a name for the group membership attribute (should not exceed 63 characters). This attribute is sent to the LDAP server when authenticating users. |
| net-time <1-10> | Optional. Select a value from 1 - 10 to configure the network timeout (number of seconds to wait for a response from the target primary or secondary LDAP server). The default is 10 seconds. |
| start-tls net-timeout <1-10> | Optional. Select a value from 1 - 10 to configure the network timeout for secure communication using start_tls support on the external LDAP server. |
| tls-mode net-timeout <1-10> | Optional. Select a value from 1 - 10 to configure the network timeout for secure communication using tls_mode support on the external LDAP server. |
## Examples

```bash
rfs7000-37FABE(config-radius-server-policy-test)#ldap-server dead-period 100
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#ldap-server primary host 172.16.10.19 port 162 login test bind-dn bind-dn1 base-dn base-dn1 passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter groupfilter1 group-membership groupmembership1 net-timeout 2
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#show context radius-server-policy test
authentication eap-auth-type tls crl-check
ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the LDAP server parameters</td>
</tr>
</tbody>
</table>
## 16.2.8 local

- **radius-server-policy**

Configures a local RADIUS realm on this RADIUS server policy

When the local RADIUS server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```
local realm <RADIUS-REALM>
```

### Parameters

- **local realm <RADIUS-REALM>**

<table>
<thead>
<tr>
<th>realm &lt;RADIUS-REALM&gt;</th>
<th>Configures a local RADIUS realm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;RADIUS-REALM&gt; – Sets a local RADIUS realm name (a string not exceeding 50 characters)</td>
</tr>
</tbody>
</table>

### Examples

```
rfs7000-37FABE(config-radius-server-policy-test)#local realm realm1
```

```
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
  authentication eap-auth-type tls
crl-check
local realm realm1
  ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
  ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#
```

### Related Commands

- **no** Removes the RADIUS local realm
16.2.9 **nas**

> **radius-server-policy**

Configures the key sent to a RADIUS client

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or Access Point managed network.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash algorithm to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified access reject message, the username and password are considered to be incorrect, and the user is not authenticated.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
nas <IP/M> secret [0|2]<LINE>
nas <IP/M> secret [0 <LINE>|2 <LINE>|<LINE>]
```

**Parameters**

- `<IP/M>`
  - Sets the RADIUS client’s IP address
    - `<IP/M>` – Sets the RADIUS client’s IP address in the A.B.C.D/M format
- `secret [0 <LINE>|2 <LINE>|<LINE>]`
  - Sets the RADIUS client’s shared secret. Use one of the following options:
    - `0 <LINE>` – Sets an UNENCRYPTED secret
    - `2 <LINE>` – Sets an ENCRYPTED secret
    - `<LINE>` – Defines the secret (client shared secret) up to 64 characters

**Examples**

```
rfs7000-37FABE(config-radius-server-policy-test)#nas 172.16.10.10/24 secret 0 wirelesswell
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
  authentication eap-auth-type tls
crl-check
  nas 172.16.10.10/24 secret 0 wirelesswell
  local realm realm1
  ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "base-dn1" passwd 0 test123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
  ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#
```

**Related Commands**

- `no` [Removes a RADIUS server’s client on a RADIUS server policy]
16.2.10 no

Negates a command or reverts back to default settings. When used with in the config RADIUS server policy mode, the no command removes settings, such as crl-check, LDAP group verification, RADIUS client etc.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
no [authentication|bypass|chase-referral|clr-check|ldap-agent|ldap-group-verification|
ladp-server|local|nas|proxy|session-resumption|termination|use]
no bypass [crl-check|expired-crl]
no authentication [data-source|eap]
no authentication [data-source {ldap {fallback}|local|ssid}|eap configuration]
no [chase-referral|clr-check|ldap-group-verification|nas <IP/M>|session-resumption]
no ldap-agent [join-retry-timeout|primary|secondary]
no local realm [<REALM-NAME>|all]
no proxy [realm <REALM-NAME>|retry-count|retry-delay]
no ldap-server [dead-period|primary|secondary]
no termination
no use [radius-group [<RAD-GROUP-NAME>|all]]|radius-user-pool-policy
[<RAD-USER-POOL-NAME>|all]]
```

Parameters
- no <PARAMETERS>

Examples
The following example shows the RADIUS server policy 'test' settings before the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
  authentication eap-auth-type tls
crl-check
  nas 172.16.10.10/24 secret 0 wirelesswell
local realm realm1
  ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
  "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
  "groupfilter1" group-membership groupmembership1 net-timeout 2
  ldap-server dead-period 100
rfs7000-37FABE(config-radius-server-policy-test)#
```

```plaintext
rfs7000-37FABE(config-radius-server-policy-test)#no authentication eap configuration
rfs7000-37FABE(config-radius-server-policy-test)#no crl-check
rfs7000-37FABE(config-radius-server-policy-test)#no local realm realm1
rfs7000-37FABE(config-radius-server-policy-test)#no nas 172.16.10.10/24
rfs7000-37FABE(config-radius-server-policy-test)#no ldap-server dead-period
```
The following example shows the RADIUS server policy 'test' settings after the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
rfs7000-37FABE(config-radius-server-policy-test)#
```
16.2.11 proxy

Configure a proxy RADIUS server based on the realm/suffix. The realm identifies where the RADIUS server forwards AAA requests for processing.

A user’s access request is sent to a proxy RADIUS server if it cannot be authenticated by the local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the proxy server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

proxy [realm|retry-count|retry-delay]

proxy realm <REALM-NAME> server <IP> port <1024-65535> secret
  [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]

proxy retry-count <3-6>

proxy retry-delay <5-10>

Parameters

- proxy realm <REALM-NAME> server <IP> port <1024-65535> secret
  [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]

<table>
<thead>
<tr>
<th>proxy realm &lt;REALM-NAME&gt;</th>
<th>Configures the realm name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;REALM-NAME&gt;</td>
<td>- Specify the realm name. The name should not exceed 50 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>server &lt;IP&gt;</th>
<th>Configures the proxy server’s IP address. This is the address of the server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>- Sets the proxy server’s IP address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port &lt;1024-65535&gt;</th>
<th>Configures the proxy server’s port. This is the TCP/IP port number for the server that acts as a data source for the proxy server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1024-65535&gt;</td>
<td>- Sets the proxy server’s port from 1024 - 65535 (default port is 1812)</td>
</tr>
</tbody>
</table>

| secret [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>] | Sets the proxy server secret string. The options are: |
|---------------------------------|----------------------------------------------------------|
| 0 <PASSWORD>                         | - Sets an UNENCRYPTED password |
| 2 <ENCRYPTED-PASSWORD>          | - Sets an ENCRYPTED password |
| <PASSWORD>                          | - Sets the proxy server shared secret value |
proxy retry-count <3-6>

Sets the proxy server's retry count. This is the maximum number of attempts made by a controller's RADIUS server to connect to the proxy server.
- <3-6> – Sets a value from 3 - 6 (default is 3 counts)

proxy retry-delay <5-10>

Sets the proxy server's retry delay count. This is the interval the controller's RADIUS server waits before making an additional connection attempt.
- <5-10> – Sets a value from 5 - 10 seconds (default is 5 seconds)

Usage Guidelines

A maximum of five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times RADIUS requests are transmitted before giving up. The timeout value defines the interval between successive retransmission of a RADIUS request (in case of no reply).

Examples

rfs7000-37FABE(config-radius-server-policy-test)#proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
rfs7000-37FABE(config-radius-server-policy-test)#proxy retry-count 4
rfs7000-37FABE(config-radius-server-policy-test)#proxy retry-delay 8
rfs7000-37FABE(config-radius-server-policy-test)#show context radius-server-policy test
  proxy retry-delay 8
  proxy retry-count 4
  proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
  ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
rfs7000-37FABE(config-radius-server-policy-test)#

Related Commands

no | Removes or resets the RADIUS proxy server’s settings
### 16.2.12 session-resumption

- **radius-server-policy**

  Enables session resumption or fast re-authentication by using cached attributes. This feature controls the volume and duration cached data is maintained by the server policy, upon termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption.

  This feature is disabled by default.

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
session-resumption {lifetime|max-entries}
```

```
session-resumption {lifetime <1-24> {max-entries <10-1024>}}|max-entries <10-1024>}
```

**Parameters**

- `session-resumption {lifetime <1-24> {max-entries <10-1024>}}|max-entries <10-1024>}`

<table>
<thead>
<tr>
<th>lifetime &lt;1-24&gt;</th>
<th>Optional. Sets the lifetime of cached entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>{max-entries &lt;10-1024&gt; }</td>
<td>• <code>&lt;1-24&gt;</code> – Specify the lifetime period from 1 - 24 hours (default is 1 hour)</td>
</tr>
<tr>
<td></td>
<td>• <code>max-entries</code> – Optional. Configures the maximum number of entries in the cache</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;10-1024&gt;</code> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>max-entries &lt;10-1024&gt;</th>
<th>Optional. Configures the maximum number of entries in the cache</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;10-1024&gt;</code> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-radius-server-policy-test)#session-resumption lifetime 10 max-entries 11
```

```
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
  proxy retry-delay 8
  proxy retry-count 4
  proxy realm test1 server 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "bas-dn1" passwd 0 test123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
  session-resumption lifetime 10 max-entries 11
rfs7000-37FABE(config-radius-server-policy-test)#
```

**Related Commands**

| no | Disables session resumption on this RADIUS server policy |
16.2.13 termination

`radius-server-policy`

Enables EAP termination on this RADIUS server policy. When enabled, EAP authentication is terminated at the controller level. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
`termination`

Parameters
None

Examples
```
nx9500-6C8809(config-radius-server-policy-test)#termination
```
```
nx9500-6C8809(config-radius-server-policy-test)#show context radius-server-policy test
termination
no bypass crl-check
```
```
nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands
```
| `no` | Disables EAP termination on this RADIUS server policy |
```
16.2.14 use

*radius-server-policy*

Defines settings used with the RADIUS server policy

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2} | radius-user-pool-policy <RAD-USER-POOL-NAME>]

**Parameters**

- use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2} | radius-user-pool-policy <RAD-USER-POOL-NAME>]

<table>
<thead>
<tr>
<th>radius-group &lt;RAD-GROUP-NAME1&gt; {RAD-GROUP-NAME2}</th>
<th>Associates a specified RADIUS group (for LDAP users) with this RADIUS server policy. You can optionally associate two RADIUS groups with one RADIUS server policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-user-pool-policy &lt;RAD-USER-POOL-NAME&gt;</td>
<td>Associates a specified RADIUS user pool with this RADIUS server policy. Specify a user pool name.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-radius-server-policy-test)#use radius-group test
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
proxy retry-delay 8
proxy retry-count 4
proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembership1 net-timeout 2
use radius-group test
session-resumption lifetime 10 max-entries 11
rfs7000-37FABE(config-radius-server-policy-test)#

**Related Commands**

| no | Disassociates a RADIUS group or a RADIUS user pool policy from this RADIUS server policy |
16.3 radius-user-pool-policy

- **RADIUS-POLICY**

Configures a RADIUS user pool policy and enters its configuration mode.

A user pool defines policies for individual user access to the internal RADIUS resources. User pool policies define unique permissions (either temporary or permanent) that control user access to the local RADIUS resources. A pool can contain a single user or multiple users.

Use the (config) instance to configure RADIUS user pool policy commands. To navigate to the radius-user-pool-policy instance, use the following commands:

```
<DEVICE>(config)#radius-user-pool-policy <POOL-NAME>
```

```
rfs7000-37FABE(config)#radius-user-pool-policy testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

```
rfs7000-37FABE(config-radius-user-pool-testuser)#?
```

Radius User Pool Mode commands:
- `duration` Set a guest user's access duration
- `no` Negate a command or set its defaults
- `user` Radius user configuration
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

The following table summarizes RADIUS user pool policy configuration commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>duration</code></td>
<td>Modifies a guest user's duration of captive-portal access</td>
<td>page 16-35</td>
</tr>
<tr>
<td><code>user</code></td>
<td>Configures the RADIUS user parameters</td>
<td>page 16-36</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negates a command or sets its default</td>
<td>page 16-39</td>
</tr>
</tbody>
</table>
16.3.1 duration

`radius-user-pool-policy`

Modifies the duration, in minutes, that a guest user can access the captive portal

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

duration <GUEST-USER-NAME> <0-525600>

**Parameters**
- duration <GUEST-USER-NAME> <0-525600>

<table>
<thead>
<tr>
<th>duration &lt;GUEST-USER-NAME&gt; &lt;0-525600&gt;</th>
<th>Modifies the duration of captive-portal access (in minutes) for the guest user identified by the &lt;GUEST-USER-NAME&gt; keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;GUEST-USER-NAME&gt; – Specify the guest user’s name.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-525600&gt; – Specify the access duration from 0 - 525600 minutes. A value of “0” indicates unlimited access. The default is 1440 minutes.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs4000-229D58(config-radius-user-pool-wdws)#show context radius-user-pool-policy wdws
  user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#

rfs4000-229D58(config-radius-user-pool-wdws)#duration guestuser1 200

rfs4000-229D58(config-radius-user-pool-wdws)#show context radius-user-pool-policy wdws
  user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-duration 200
rfs4000-229D58(config-radius-user-pool-wdws)#
```
16.3.2 user

Configure RADIUS user parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>
{group <RAD-GROUP-NAME>} {guest}
```

```
user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>
{group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date <MM/DD/YYYY>
{access-duration <0-525600>|data-limit|email-id <EMAIL-ID>|start-time <HH:MM>
start-date <MM/DD/YYYY>|telephone <TELEPHONE-NUMBER>}
```

Parameters

- user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>
{group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date <MM/DD/YYYY>
{access-duration <0-525600>|data-limit <1-102400> committed-downlink <100-1000000>
committed-uplink <100-1000000> reduced-downlink <100-1000000> reduced-uplink
<100-1000000>|email-id <EMAIL-ID>|start-time <HH:MM> start-date <MM/DD/YYYY>
telephone <TELEPHONE-NUMBER>}
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user &lt;USERNAME&gt;</td>
<td>Adds a new RADIUS user to the RADIUS user pool</td>
</tr>
<tr>
<td>passwd</td>
<td>Configures the user password (provide a password unique to this user)</td>
</tr>
<tr>
<td>group &lt;RAD-GROUP-NAME&gt;</td>
<td>Optional. Configures the RADIUS server group of which this user is a member</td>
</tr>
<tr>
<td>guest</td>
<td>Optional. Specifies that this user is a guest user. Guest users have restricted access. After enabling a guest user account, specify the expiry time and date for this account.</td>
</tr>
<tr>
<td>expiry-time <a href="">HH:MM</a></td>
<td>Specify the user account expiry time in the HH:MM format (for example, 12:30 means 30 minutes after 12:00 the user login will expire).</td>
</tr>
</tbody>
</table>

Note: The username is a unique alphanumeric string identifying this user, and cannot be modified with the rest of the configuration.
expiry-date <MM:DD:YYYY>

Specify the user account expiry date in the MM:DD:YYYY format (for example, 02:15:2014).

{access-duration <0-525600>|data-limit <1-102400>
committed-downlink <100-1000000>
committed-uplink <100-1000000>
reduced-downlink <100-1000000>
reduced-uplink <100-1000000>
email-id <EMAIL-ID>
start-time <HH:MM>
start-date <MM:DD:YYY>
telephone <TELEPHONE-NUMBER>}

After configuring the above user details, optionally configure the following user information:

• access-duration <0-525600> – Configures the duration, in minutes, for which this guest user can access the captive portal.
• <0-525600> – Specify a value from 0 - 525600 minutes.
• data-limit <1-102400> – Configures the data limit for which this guest user can access the captive portal. Specify a value from 1 - 102400 bytes.
• committed-downlink <100-1000000> – Configures committed downlink bandwidth until data limit is reached. This value represents the download speed (in kilobits per second) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced downlink rate (specified using this command). Specify a value from 100 - 1000000 Kbps.
• committed-uplink <100-1000000> – Configures committed uplink bandwidth until data limit is reached. This value represents the upload speed (in kilobits per second) allocated to the guest user. When bandwidth is available, the user can upload data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced uplink rate (specified using this command). Specify a value from 100 - 1000000 Kbps.
• reduced-downlink <100-1000000> – Configures reduced downlink bandwidth after data limit is reached. This value represents the reduced speed the guest utilizes (in kilobits per second) when exceeding the specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced downlink rate specified here. Specify a value from 100 - 1000000 Kbps.
• reduced-uplink <100-1000000> – Configures reduced uplink bandwidth after data Limit is reached. This value represents the reduced speed the guest utilizes (in kilobits per second) when exceeding the specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced uplink rate specified here. Specify a value from 100 - 1000000 Kbps.

• email-id – Optional. User’s e-mail ID

• start-time – Optional. User’s account activation time. After specifying the activation time, specify the activation date.
• start-date – User’s account activation date

• telephone – Optional. User’s telephone number (should include the area code)

Note: To view access details of guest users on a RADIUS server, in the Priv Executable Configuration mode, use the following command:

```
show > radius > guest-users
rfs7000-37FABE#show radius guest-users time
  TIME (min:sec)
  USED    REMAINING    GUEST USER
  0:00     500:00       user1
Current time: 09:03:07
rfs7000-37FABE#
```
Examples

rfs4000-229D58(config-radius-user-pool-wdws)#user guestuser1 password 0 guestuser@1
group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#

rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#

nx4500-5CFA2B(config-radius-user-pool-pool1)#user word password 0 word group group1 guest expiry-time 11:10 expiry-date 12/12/2014 data-limit 10 committed-downlink 103 committed-uplink 100 reduced-downlink 102 reduced-uplink 101
nx4500-5CFA2B(config-radius-user-pool-pool1)#

Related Commands

| no | Deletes a user from a RADIUS user pool |
### 16.3.3 no

*radius-user-pool-policy*

Negates a command or sets its default. When used in the RADIUS user pool policy mode, the `no` command deletes a user from a RADIUS user pool.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no user <USERNAME>
```

**Parameters**

- `no user <USERNAME>`

**Examples**

The following example shows the RADIUS user pool 'wdws' settings before the 'no' command is executed:

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
  user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#
```

```
rfs4000-229D58(config-radius-user-pool-wdws)#no user guestuser1
```

The following example shows the RADIUS user pool 'wdws' settings after the 'no' command is executed:

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
rfs4000-229D58(config-radius-user-pool-wdws)#
```

**Related Commands**

- `user` Configures the RADIUS user parameters
CHAPTER 17
RADIO-QOS-POLICY

This chapter summarizes the radio QoS policy in the CLI command structure.

Configuring and implementing a radio QoS policy is essential for WLANs with heavy traffic and less bandwidth. The policy enables you to provide preferential service to selected network traffic by controlling bandwidth allocation. The radio QoS policy can be applied to VLANs configured on an access point. In case no VLANs are configured, the radio QoS policy can be applied to an access point's Ethernet and radio ports.

Without a dedicated QoS policy, a network operates on a best-effort delivery basis, meaning all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy’s intended wireless client base.

A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.

Within a managed wireless network, wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined Enhanced Distributed Channel Access (EDCA) mechanisms stating high priority traffic can access the network sooner then lower priority traffic. The EDCA defines four traffic classes (or access categories); voice (highest), video (next highest), best effort, and background (lowest). The EDCA has defined a time interval for each traffic class, known as the Transmit Opportunity (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported.

IEEE 802.11e includes an advanced power saving technique called Unscheduled Automatic Power Save Delivery (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as bursts, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created Wireless Multimedia (WMM) and WMM Power Save (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. A managed wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.
Enabling WMM support on a WLAN just advertises the WLAN’s WMM capability and radio configuration to wireless clients. The wireless clients must also support WMM and use the values correctly while accessing the WLAN to benefit.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected access point radios and their wireless clients. Parameters impacting access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN’s WMM settings.

Wireless network controllers (access points, controllers, and service platforms) include a Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP) and Application Layer Gateway (ALG) enabling devices to identify voice streams and dynamically set voice call bandwidth.

Wireless network controllers also support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN’s WMM access control setting.

**NOTE:** Statistically setting a WLAN WMM access category value only prioritizes traffic to the client.

Wireless network administrators can also assign weights to each WLAN in relation to user priority levels. The lower the weight, the lower the priority. Use a weighted technique to achieve different QoS levels across WLANs.

All devices rate-limit bandwidth for WLAN sessions. This form of per-user rate limiting enables administrators to define uplink and downlink bandwidth limits for users and clients. This sets the level of traffic a user or client can forward and receive over the WLAN. If the user or client exceeds the limit, excessive traffic is dropped.

Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using Vendor Specific Attributes (VSAs). Rate limits can be applied to users authenticating using 802.1X, captive portal authentication, and devices using MAC authentication.

Use the (config) instance to configure radios QoS policy related configuration commands. To navigate to the radio QoS policy instance, use the following commands:

```plaintext
<DEVICE>(config)#radio-qos-policy <POLICY-NAME>
```

```plaintext
rfs7000-37FABE(config)#radio-qos-policy test
rfs7000-37FABE(config-radio-qos-test)#?
```

**Radio QoS Mode commands:**
- accelerated-multicast: Configure multicast streams for acceleration
- admission-control: Configure admission-control on this radio for one or more access categories
- no: Negate a command or set its defaults
- smart-aggregation: Configure smart aggregation parameters
- wmm: Configure 802.11e/Wireless MultiMedia parameters
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

```plaintext
rfs7000-37FABE(config-radio-qos-test)#
```
NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
17.1 radio-qos-policy

The following table summarizes radio QoS policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Configures multicast streams for acceleration</td>
<td>page 17-5</td>
</tr>
<tr>
<td>admission-control</td>
<td>Enables admission control across all radios for one or more access categories</td>
<td>page 17-6</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or resets configured settings to their default</td>
<td>page 17-9</td>
</tr>
<tr>
<td>smart-aggregation</td>
<td>Configures smart aggregation parameters</td>
<td>page 17-11</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands in the radio QoS configuration mode</td>
<td>page 17-13</td>
</tr>
<tr>
<td>wmm</td>
<td>Configures 802.11e/wireless multimedia parameters</td>
<td>page 17-14</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
17.1.1 accelerated-multicast

`radio-qos-policy`

Configures multicast streams for acceleration. Multicasting allows group transmission of data streams.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
accelerated-multicast [client-timeout|max-client-streams|max-streams|overflow-policy|stream-threshold]
```

```
```

**Parameters**


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-timeout</td>
<td>Configures a timeout period in seconds for wireless clients</td>
</tr>
<tr>
<td>&lt;5-6000&gt;</td>
<td>- Specify a value from 5 - 6000 seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>max-client-streams</td>
<td>Configures the maximum number of accelerated multicast streams per client</td>
</tr>
<tr>
<td>&lt;1-4&gt;</td>
<td>- Specify a value from 1 - 4. The default is 2.</td>
</tr>
<tr>
<td>max-streams</td>
<td>Configures the maximum number of accelerated multicast streams per radio</td>
</tr>
<tr>
<td>&lt;0-256&gt;</td>
<td>- Specify a value from 0 - 256. The default is 25.</td>
</tr>
<tr>
<td>overflow-policy</td>
<td>Specifies the policy in case too many clients register simultaneously.</td>
</tr>
<tr>
<td>[reject</td>
<td>revert]</td>
</tr>
<tr>
<td></td>
<td>- revert – Reverts to regular multicast delivery</td>
</tr>
<tr>
<td>stream-threshold</td>
<td>Configures the number of multicast packets per second threshold value. Once</td>
</tr>
<tr>
<td>&lt;1-500&gt;</td>
<td>this threshold is crossed, the system triggers streams to accelerate.</td>
</tr>
<tr>
<td></td>
<td>- Specify a value from 1 - 500. The default is 25 packets per second.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-radio-qos-test)#accelerated-multicast client-timeout 500
rfs7000-37FABE(config-radio-qos-test)#accelerated-multicast stream-threshold 15
```

```
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
accelerated-multicast stream-threshold 15
accelerated-multicast client-timeout 500
rfs7000-37FABE(config-radio-qos-test)#
```

**Related Commands**

`no` Reverts accelerated multicasting settings to their default
17.1.2 admission-control

*radio-qos-policy*

Enables admission control across all radios for one or more access categories. Enabling admission control for an access category, ensures clients associated to an access point and complete WMM admission control before using that access category.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

admission-control [background|best-effort|firewall-detected-traffic|implicit-tspec|video|voice]

admission-control [firewall-detected-traffic|implicit-tspec]

admission-control [background|best-effort|video|voice] {max-airtime-percent|max-clients|max-roamed-clients|reserved-for-roam-percent}

admission-control [background|best-effort|video|voice] {max-airtime-percent <0-150>|max-clients <0-256>|max-roamed-clients <0-256>|reserved-for-roam-percent <0-150>}

**Parameters**

- admission-control [firewall-detected-traffic|implicit-tspec]

| admission-control firewall-detected-traffic | Enforces admission control for traffic whose access category is detected by the firewall ALG. For example, SIP voice calls. This feature is enabled by default. When enabled, the firewall simulates reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TSPEC frames only. |
| admission-control implicit-tspec | Enables implicit traffic specifiers for clients that do not support WMM TSPEC, but are accessing admission-controlled access categories. This feature is enabled by default. This feature requires wireless clients to send their traffic specifications to an access point before they can transmit or receive data. If enabled, this setting applies to this radio QoS policy. When enabled, the access point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TSPEC frames only. |

| admission-control [background|best-effort|video|voice] {max-airtime-percent <0-150>|max-clients <0-256>|max-roamed-clients <0-256>|reserved-for-roam-percent <0-150>} | |

<p>| admission-control background | Configures background access category admission control parameters |
| admission-control best-effort | Configures best effort access category admission control parameters |
| admission-control video | Configures video access category admission control parameters |</p>
<table>
<thead>
<tr>
<th>admission-control voice</th>
<th>Configures voice access category admission control parameters</th>
</tr>
</thead>
</table>
| max-airtime-percent <0-150> | Optional. Specifies the maximum percentage of airtime, including oversubscription, for the following access category:  
  - background – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for low (background) client traffic. Background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved to support background data.  
  - best-effort – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for normal (best-effort) client traffic. Normal best effort traffic needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for best effort data support.  
  - video – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for voice supported client traffic. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video.  
  - voice – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for voice supported client traffic. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice.  
  The following keyword is common to all of the above traffic types:  
  - <0-150> – Specify a value from 0 - 150. This is the maximum percentage of airtime, including oversubscription, for the selected access category. The default is 75%. |
| max-clients <0-256> | Optional. Specifies the maximum number of wireless clients admitted to the following access categories:  
  - background – Sets the number of wireless clients supporting low (background) traffic allowed to exist (and consume bandwidth) within the radio’s QoS policy  
  - best-effort – Sets the number of wireless clients supporting normal (best-effort) traffic allowed to exist (and consume bandwidth) within the radio’s QoS policy  
  - video – Sets the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio’s QoS policy.  
  - voice – Sets the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio’s QoS policy.  
  Note: Since voice and video supported wireless clients use a greater portion of a controller’s resources than lower bandwidth traffic (like low and best effort categories), consider setting the max-client value proportionally to the number of other QoS policies supporting voice access category clients.  
  The following keyword is common to all of the above traffic types:  
  - <0-256> – Specify a value from 0 - 256. This is the maximum number of wireless clients admitted to the selected access category. The default is 100 clients. |
max-roamed-clients <0-256>  Optional. Specifies the maximum number of roaming wireless clients admitted to the selected access category
   • background – Sets the number of low (background) supported wireless clients allowed to roam to a different access point radio
   • best-effort – Sets the number of normal (best-effort) supported wireless clients allowed to roam to a different access point radio
   • video – Sets the number of video supported wireless clients allowed to roam to a different access point radio
   • voice – Sets the number of voice supported wireless clients allowed to roam to a different access point radio

The following keyword is common to all of the above traffic types:
   • <0-256> – Specify a value from 0 - 256. This is the maximum number of roaming wireless clients admitted to the selected access category. The default is 10 roamed clients.

reserved-for-roam-percent <0-150>  Optional. Calculates the percentage of air time, including oversubscription, allocated exclusively for roaming clients. This value is calculated relative to the configured max air time for this access category.
   • background – Sets the roam utilization (in the form of a percentage of the radio’s bandwidth) allotted to admission control for low (background) supported clients who have roamed to a different radio.
   • best-effort – Sets the roam utilization (in the form of a percentage of the radio’s bandwidth) allotted to admission control for normal (best-effort) supported clients who have roamed to a different radio.
   • video – Sets the roam utilization (in the form of a percentage of the radio’s bandwidth) allotted to admission control for video supported clients who have roamed to a different radio.
   • voice – Sets the roam utilization (in the form of a percentage of the radio’s bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio.

The following keyword is common to all of the above traffic types:
   • <0-150> – Specify a value from 0 - 150. This is the percentage of air time, including oversubscription, allocated exclusively for roaming clients associated with the selected access category. The default is 10%.

Examples

```bash
rfs7000-37FABE(config-radio-qos-test)#admission-control best-effort max-clients 200
rfs7000-37FABE(config-radio-qos-test)#admission-control voice reserved-for-roam-percent 8
rfs7000-37FABE(config-radio-qos-test)#admission-control voice max-airtime-percent 9
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
   admission-control voice max-airtime-percent 9
   admission-control voice reserved-for-roam-percent 8
   admission-control best-effort max-clients 200
   accelerated-multicast stream-threshold 15
   accelerated-multicast client-timeout 500
rfs7000-37FABE(config-radio-qos-test)#
```

Related Commands

```none
no
```
Reverts or resets admission control settings to their default
17.1.3 no

Negates a command or resets configured settings to their default. When used in the radio QOS policy mode, the no command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
no [accelerated-multicast|admission-control|smart-aggregation|wmm|service]

no accelerated-multicast [client-timeout|max-client-streams|max-streams|
  overflow-policy|stream-threshold]

no admission-control [firewall-detected-traffic|implicit-tspec|background|
  best-effort|video|voice]

no admission-control [firewall-detected-traffic|implicit-tspec]

no admission-control [background|best-effort|video|voice] {max-airtime-percent|
  max-clients|max-roamed-clients|reserved-for-roam-percent}

no smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}

no smart-aggregation {delay [background|best-effort|streaming-video|
  video-conferencing|voice] |max-mesh-hops|min-aggregation-limit}

no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]

no service admission-control across-reassoc
```

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Negates a command or resets configured settings to their default. When used in the radio QOS policy mode, the no command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters. |

Examples

The following example shows the Radio-qos-policy ‘test’ settings before the ‘no’ commands are executed:

```plaintext
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
  admission-control voice max-airtime-percent 9
  admission-control voice reserved-for-roam-percent 8
  admission-control best-effort max-clients 200
  accelerated-multicast stream-threshold 15
  accelerated-multicast client-timeout 500

rfs7000-37FABE(config-radio-qos-test)#

rfs7000-37FABE(config-radio-qos-test)#no admission-control best-effort max-clients
rfs7000-37FABE(config-radio-qos-test)#no accelerated-multicast client-timeout
```
The following example shows the Radio-qos-policy 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
  admission-control voice max-airtime-percent 9
  admission-control voice reserved-for-roam-percent 8
  accelerated-multicast stream-threshold 15
rfs7000-37FABE(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
  service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#no service admission-control across-reassoc

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
rfs4000-229D58(config-radio-qos-test)#
```
### 17.1.4 smart-aggregation

- **radio-qos-policy**

Configures smart aggregation parameters on this Radio QoS policy

Smart aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame’s typical aggregation, an aggregated frame is sent when:

- A pre-configured number of aggregated frames is reached
- An administrator-defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- An administrator-defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic might not be aggregated, but sent immediately. Whereas, background data traffic is set a delay for aggregating frames, and these aggregated frames are sent.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

- `smart-aggregation {delay/max-mesh-hops/min-aggregation-limit}
- smart-aggregation {delay [background|best-effort|streaming-video|video-conferencing|voice] <0-1000>}
- smart-aggregation {max-mesh-hops <1-10>}
- smart-aggregation {min-aggregation-limit <0-64>}

**Parameters**

- `smart-aggregation {delay [background|best-effort|streaming-video|video-conferencing|voice] <0-1000>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay</td>
<td>Optional. Configures the maximum delay parameter for each traffic type. This is the maximum delay, in milliseconds, in the transmission of the first frame received.</td>
</tr>
<tr>
<td>background</td>
<td>Configures the maximum delay parameter, in milliseconds, for background traffic (250 msec)</td>
</tr>
<tr>
<td>best-effort</td>
<td>Configures the maximum delay parameter, in milliseconds, for best effort traffic (150 msec)</td>
</tr>
<tr>
<td>streaming-video</td>
<td>Configures the maximum delay parameter, in milliseconds, for streaming video traffic (150 msec)</td>
</tr>
<tr>
<td>video-conferencing</td>
<td>Configures the maximum delay parameter, in milliseconds, for video conference traffic (40 msec)</td>
</tr>
<tr>
<td>voice</td>
<td>Configures the maximum delay parameter, in milliseconds, for voice traffic (0 msec)</td>
</tr>
<tr>
<td>&lt;0-1000&gt;</td>
<td>This parameter is common to all of the above traffic types.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-1000&gt; – Specify a value from 0 - 1000 msec.</td>
</tr>
</tbody>
</table>
### smart-aggregation \( \text{max-mesh-hops} \ <1-10> \)

<table>
<thead>
<tr>
<th>max-mesh-hops &lt;1-10&gt;</th>
<th>Optional. Sets the maximum number of expected hops to the destination within a mesh</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-10&gt; – Specify a value from 1 - 10. The default is 3 hops.</td>
</tr>
</tbody>
</table>

### smart-aggregation \( \text{min-aggregation-limit} \ <0-64> \)

<table>
<thead>
<tr>
<th>min-aggregation-limit &lt;0-64&gt;</th>
<th>Optional. Sets the minimum number of aggregates buffered before an aggregate is sent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;0-64&gt; – Specify a value from 0 - 64. The default is 8 frames.</td>
</tr>
</tbody>
</table>

### Examples

```
rfs7000-37FABE(config-radio-qos-test)#smart-aggregation delay voice 50
```

```
rfs7000-37FABE(config-radio-qos-test)#smart-aggregation delay background 100
```

```
rfs7000-37FABE(config-radio-qos-test)#show context radio-qos-policy test
  smart-aggregation delay voice 50
  smart-aggregation delay background 100
rfs7000-37FABE(config-radio-qos-test)#
```

### Related Commands

```
no
```

- Resets the minimum aggregation limit
17.1.5 service

Invokes service commands in the radio QoS configuration mode

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

service [admission-control|show]

service admission-control across-reassoc

service show cli

Parameters

- service admission-control across-reassoc

- service show cli

Examples

rfs4000-229D58(config-radio-qos-test)#service admission-control across-reassoc

rfs4000-229D58(config-radio-qos-test)#show context radio-qos-policy test

rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#service show cli

Radio QoS Mode mode:

+-help [help]
  +--search
    +-WORD [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-detailed [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-only-show [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-skip-show [help search WORD ([detailed|only-show|skip-show|skip-no])
    +-skip-no [help search WORD ([detailed|only-show|skip-show|skip-no])
  +-show
    +-commands [show commands]
    +-adoption
    +-log

--More--

Related Commands

do

Disables retention of previously negotiated TSPEC parameters across re-associations on the radio
17.1.6 wmm

Configures 802.11e wireless multimedia (wmm) parameters

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
wmm [background|best-effort|video|voice]
wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```

Parameters

- wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]

<table>
<thead>
<tr>
<th>wmm background</th>
<th>Configures background access category wireless multimedia settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>wmm best-effort</td>
<td>Configures best effort access category wireless multimedia settings</td>
</tr>
<tr>
<td>wmm video</td>
<td>Configures video access category wireless multimedia settings</td>
</tr>
<tr>
<td>wmm voice</td>
<td>Configures voice access category wireless multimedia settings</td>
</tr>
<tr>
<td>aifsn &lt;1-15&gt;</td>
<td>Configures Arbitrary Inter-Frame Space Number (AIFSN) as the wait time between data frames derived from the AIFSN and slot time</td>
</tr>
<tr>
<td></td>
<td>background – Sets the current AIFSN for low (background) traffic. The default is 7.</td>
</tr>
<tr>
<td></td>
<td>best-effort – Sets the current AIFSN for normal (best-effort) traffic. The default is 3.</td>
</tr>
<tr>
<td></td>
<td>video – Set the current AIFSN for video traffic. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1.</td>
</tr>
<tr>
<td></td>
<td>voice – Sets the current AIFSN for voice traffic. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1.</td>
</tr>
<tr>
<td></td>
<td>The following keyword is common to all of the above traffic types:</td>
</tr>
<tr>
<td></td>
<td>&lt;1-15&gt; – Sets a value from 1 - 15</td>
</tr>
<tr>
<td>cw-max &lt;0-15&gt;</td>
<td>Clients pick a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window.</td>
</tr>
<tr>
<td></td>
<td>background – Sets CW Max for low (background) traffic. The default is 10.</td>
</tr>
<tr>
<td></td>
<td>best-effort – Sets CW Max for normal (best effort) traffic. The default is 6.</td>
</tr>
<tr>
<td></td>
<td>voice – Sets CW Max for voice traffic. The default is 3.</td>
</tr>
<tr>
<td></td>
<td>video – Sets CW Max for video traffic. The default is 4</td>
</tr>
</tbody>
</table>

Contd..
### Usage Guidelines

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client, and WLAN is required to support WMM.
- WMM enabled clients can co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a Best Effort access category.
- Default WMM values are recommended for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.
- Overloading an access point radio with too much high priority traffic (especially voice) degrades overall service quality for all users.
- TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TSPEC or even support WMM traffic prioritization.

### CW-Min <0-15>

Clients select a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window.

- **background** – Sets CW Min for low (background) traffic. The default is 4.
- **best-effort** – Sets CW Min for normal (best effort) traffic. The default is 4.
- **voice** – Sets CW Min for voice traffic. The default is 2.
- **video** – Sets CW Min for video traffic. The default is 3.

### TXOP-Limit <0-65535>

Set the interval, in microseconds, during which a particular client has the right to initiate transmissions:

- **background** – Sets TXOP for low (background) traffic. The default is 0.
- **best-effort** – Sets TXOP for normal (best effort) traffic. The default is 4.
- **voice** – Sets TXOP for voice traffic. The default is 47.
- **video** – Sets TXOP for video traffic. The default is 94.

### Key Terms

The following keyword is common to all of the above traffic types:

- **ECW**: the contention window. The actual value used is \((2^{\text{ECW}} - 1)\).
  
  **Note:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).
Examples

rfs7000-37FABE(config-radio-qos-test)#wmm best-effort aifsn 7
rfs7000-37FABE(config-radio-qos-test)#wmm voice txop-limit 1

rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
  wmm best-effort aifsn 7
  wmm voice txop-limit 1
  admission-control voice max-airtime-percent 9
  admission-control voice reserved-for-roam-percent 8
  accelerated-multicast stream-threshold 15
rfs7000-37FABE(config-radio-qos-test)#

Related Commands

| no          | Reverts or resets 802.11e/wireless multimedia settings to their default |
This chapter summarizes the role policy commands in the CLI command structure.

A well defined role policy simplifies user management, and is a significant aspect of WLAN management. It acts as a role based firewall (much like ACLs) consisting of user-defined roles. Each role has a set of match criteria (filters) used to filter wireless clients. The action taken when a client matches the defined filters, is determined by the IP or MAC ACL associated with the user-defined role. Based on the conditions specified in the IP and/or MAC ACL, clients are granted or denied access to the controller managed network. The role policy also defines the VLAN and data rates assigned to clients provided network access.

A role policy also enables LDAP service, allowing controllers and access points to retrieve user information from the LDAP server. This information is matched with the user-defined role filters to determine if a client matches the role or not, and should be allowed or denied access to the controller managed network.

Use the (config-role-policy) instance to configure role policy related configuration commands. To navigate to the config-role instance, use the following commands:

```
<DEVICE>(config)#role-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#role-policy test
rfs7000-37FABE(config-role-policy-test)#?
```

Role Policy Mode commands:

- `default-role`  Configuration for Wireless Clients not matching any role
- `ldap-deadperiod`  Ldap dead period interval
- `ldap-query`  Set the ldap query mode
- `ldap-server`  Add a ldap server
- `ldap-timeout`  Ldap query timeout interval
- `no`  Negate a command or set its defaults
- `user-role`  Create a role

- `clrscr`  Clears the display screen
- `commit`  Commit all changes made in this session
- `do`  Run commands from Exec mode
- `end`  End current mode and change to EXEC mode
- `exit`  End current mode and down to previous mode
- `help`  Description of the interactive help system
- `revert`  Revert changes
- `service`  Service Commands
- `show`  Show running system information
- `write`  Write running configuration to memory or terminal
NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
18.1 role-policy

The following table summarizes role policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-role</td>
<td>Assigns the default role to clients not matching any of the user-defined roles defined in the role policy</td>
<td>page 18-4</td>
</tr>
<tr>
<td>ldap-deadperiod</td>
<td>Configures the Lightweight Directory Access Protocol (LDAP) deadperiod interval</td>
<td>page 18-6</td>
</tr>
<tr>
<td>ldap-query</td>
<td>Enables LDAP service and specifies the LDAP server query mode</td>
<td>page 18-7</td>
</tr>
<tr>
<td>ldap-server</td>
<td>Configures the LDAP server settings</td>
<td>page 18-8</td>
</tr>
<tr>
<td>ldap-timeout</td>
<td>Configures the LDAP query timeout interval</td>
<td>page 18-10</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 18-11</td>
</tr>
<tr>
<td>user-role</td>
<td>Creates a role and associates it to the newly created role policy</td>
<td>page 18-12</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
18.1.1 default-role

role-policy

Assigns a default role to a wireless client that fails to match any of the user-defined roles.

When a wireless client accesses a network, the client’s details, retrieved from the LDAP server, are matched against all user-defined roles within the role policy. If the client fails to match any of these user-defined role filters, the client is assigned the default role. The action taken (permit or deny access) is determined by the IP and/or MAC ACL associated with the default role.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

default-role use [ip-access-list|ipv6-access-list|mac-access-list]
default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
   <IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>

Parameters

- default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
  <IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>

**default-role use** Enables default role configuration. This role is applied to a wireless client not matching any of the user-defined roles.

- Use – Associates an IP, IPv6, or MAC access list with the default role

**[ip-access-list|ipv6-access-list|mac-access-list] [in|out] <IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>**

Associates an IP access list, IPv6 access list, or a MAC access list with this default role.

- in – Applies the rule (IP, IPv6, or MAC) to incoming packets
- out – Applies the rule (IP, IPv6, or MAC) to outgoing packets

**Note:** IP and MAC *access control lists* (ACLs) act as firewalls by blocking and/or permitting data traffic in both directions (inbound and outbound) within a managed network. IP ACLs use IP addresses for matching operations. Whereas, MAC ACLs use MAC addresses for matching operations. In case of a match (i.e. if a packet is received from or is destined for a specified IP or MAC address), an action is taken. This action is a typical allow, deny or mark designation to controller packet traffic. For more information on ACLs, see ACCESS-LIST.

- <IP/IPv6/MAC-ACCESS-LIST-NAME> – Specify the access list name.

**Note:** The ACL applied determines the action applied to a client assigned the default role.

**precedence <1-100>** The following keyword is common to the all of the above parameters:

- precedence – Assigns a precedence value to the ACL identified in the previous step.
- <1-100> – Specify a precedence from 1 - 100.

**Note:** ACLs are applied in increasing order of their precedence. Rules with lower precedence are given priority.
Examples

rfs7000-37FABE(config-role-policy-test)#default-role use ip-access-list in test precedence 1

rfs7000-37FABE(config-role-policy-test)#show context role-policy test
  default-role use ip-access-list in test precedence 1
rfs7000-37FABE(config-role-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes or resets the default role configuration</td>
</tr>
</tbody>
</table>
### 18.1.2 ldap-deadperiod

 role-policy

Configures the LDAP deadperiod interval

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ldap-deadperiod <60-300>

**Parameters**

- ldap-deadperiod <60-300>

<table>
<thead>
<tr>
<th>ldap-deadperiod &lt;60-300&gt;</th>
<th>Configures a LDAP dead period. When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details to match with user-defined role filters. The LDAP deadperiod is the interval between two consecutive attempts to bind with the LDAP server. To enable LDAP service, use the ldap-query command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;60-300&gt; – Specify the interval from 60 - 300 seconds. The default is 120 seconds.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-role-policy-test)#ldap-deadperiod 100

rfs7000-37FABE(config-role-policy-test)#show context role-policy test
default-role use ip-access-list in test precedence 1

ldap-deadperiod 100

rfs7000-37FABE(config-role-policy-test)#

**Related Commands**

- **no** Removes or resets the LDAP deadperiod interval
18.1.3 ldap-query

Enables LDAP service and specifies the LDAP server query mode

Configuring the LDAP server query mode automatically enables LDAP service on this role policy. By default LDAP service is disabled.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
ldap-query [self|through-controller]

Parameters
- ldap-query [self|through-controller]

<table>
<thead>
<tr>
<th>self</th>
<th>Configures LDAP query mode as self. The AP directly queries the LDAP server for user information. Select ‘self’ to use local LDAP server resources configured using the ldap-server command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>through-controller</td>
<td>Configures LDAP query mode as through-controller. The AP queries the LDAP server, for user information, through the controller. <strong>Note:</strong> Use this option when the AP is layer 2 adopted to the controller.</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-role-policy-test)#ldap-query self
rfs7000-37FABE(config-role-policy-test)#show context role-policy test
default-role use ip-access-list in test precedence 1
ldap-query self
ldap-deadperiod 100
rfs7000-37FABE(config-role-policy-test)#

Related Commands
- no Disables LDAP service on this role policy
18.1.4 ldap-server

Associates a specified LDAP server with this role policy. Use this command to configure the credentials needed to bind with the LDAP server.

When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details. This information is matched with the user-defined roles within the role policy. If a match is made, the user is assigned the role and allowed or denied access to the controller managed network.

You can associate two LDAP servers with a role policy, allowing failover in case the primary server is unreachable.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ldap-server <1-2> host [<IP>|<FQDN>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>} {server-type [active-directory|openldap]}
```

Parameters

- ldap-server <1-2> Specify the LDAP server ID from 1 - 2.
- host [<IP>|<FQDN>] Specify the LDAP server’s IP address or Fully Qualified Domain Name (FQDN).
- bind-dn <BIND-DN> Specify the bind distinguished name (used for binding with the server).
- base-dn <BASE-DN> Specify the base distinguished name (used for searching). This should not exceed 127 characters.
- bind-password <PASSWORD> Specify the LDAP server password associated with the bind DN.
- port <1-65535> Optional. Specify the LDAP server port from 1 - 65535. (default is 389).
- server-type [active-directory|openldap] The following keywords are common to the ‘port’ parameter:
  - server-type – Optional. Specifies the LDAP server type
    - active-directory – Enables support for active directory attribute search. This is the default setting.
    - openldap – Enables support for openLDAP attribute search

Usage Guidelines

Use the ldap-query command to enable LDAP service on a role policy.

Use the show > role > ldap-stats command to view LDAP server status and state.
Examples
rfs7000-37FABE(config-role-policy-test)#ldap-server 1 host 192.168.13.7 bind-dn "CN=Administrator,CN=Users,DC=TechPub,DC=com" base-dn "CN=Administrator,CN=Users,DC=TechPub,DC=com" bind-password 0 superuser port 2
rfs7000-37FABE(config-role-policy-test)#
rfs7000-37FABE(config-role-policy-test)#show context role-policy test
default-role use ip-access-list in test precedence 1
ldap-query self
ldap-deadperiod 100
ldap-server 1 host 192.168.13.7 bind-dn CN=Administrator,CN=Users,DC=TechPub,DC=com base-dn CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
rfs7000-37FABE(config-role-policy-test)#

Related Commands

| no | Removes or resets the LDAP server settings |
### 18.1.5 ldap-timeout

**role-policy**

Configures the LDAP timeout interval. This is the interval after which a LDAP query is timed out.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
ldap-timeout <1-5>
```

**Parameters**

- `ldap-timeout <1-5>`

**Examples**

```plaintext
rfs7000-37FABE(config-role-policy-test)#ldap-timeout 1
```

```plaintext
rfs7000-37FABE(config-role-policy-test)#show context
role-policy test default-role use ip-access-list in test precedence 1
ldap-query self
ldap-timeout 1
ldap-deadperiod 100
ldap-server 1 host 192.168.13.7 bind-dn CN=Administrato,DC=TechPub,DC=com base-dn CN=Administrator,DC=Users,DC=com bind-password 0 superuser port 2
rfs7000-37FABE(config-role-policy-test)#
```

**Related Commands**

- `no` Removes or resets the LDAP query timeout to default (2 seconds)
18.1.6 no

Negates a command or resets settings to their default. When used in the config role policy mode, the no command removes or resets the role policy settings.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [default-role|ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout|user-role]
no [ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout]
no default-role use [ip-access-list|ipv6-access-list|mac-access-list]
no default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>

Parameters

- no <PARAMETERS>

Examples

The following example shows the role policy 'test' setting before the 'no' commands are executed:

```
rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
  default-role use ip-access-list in test precedence 1
  ldap-query self
  ldap-timeout 1
  ldap-deadperiod 100
  ldap-server 1 host 192.168.13.7 bind-dn CN=Administrat, CN=Users, DC=TechPub, DC=com
  base-dn CN=Administrat, CN=Users, DC=com bind-password 0 superuser port 2
```

```
rfs7000-37FABE(config-role-policy-test)#no ldap-deadperiod
rfs7000-37FABE(config-role-policy-test)#no ldap-timeout
rfs7000-37FABE(config-role-policy-test)#no ldap-server 1
```

The following example shows the role policy 'test' setting after the 'no' commands are executed:

```
rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
  default-role use ip-access-list in test precedence 1
  ldap-query self
```

```
rfs7000-37FABE(config-role-policy-test)#no ldap-deadperiod
rfs7000-37FABE(config-role-policy-test)#no ldap-timeout
rfs7000-37FABE(config-role-policy-test)#no ldap-server 1
```
18.1.7 user-role

role-policy

This command creates a user-defined role. Each user-defined role has a set of Active Directory attributes. Each attribute is matched against the information returned by the LDAP server, until a complete match of role is found. The following table summarizes user role configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-role</td>
<td>Creates a new user role and enters its configuration mode</td>
<td>18-13</td>
</tr>
<tr>
<td>user-role commands</td>
<td>Summarizes user role configuration mode commands</td>
<td>18-15</td>
</tr>
</tbody>
</table>

Table 18.2 User-Role-Config Commands
18.1.7.1 user-role

- **user-role**

Creates a user-defined role. Each role consists of a set of filters and action. The filters are match criteria used to filter wireless clients. And the action defines the action taken when a client matches the specified filters.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`user-role <ROLE-NAME> precedence <1-10000>`

**Parameters**

- `user-role <ROLE-NAME> precedence <1-10000>`

**Examples**

```
rfs7000-37FABE(config-role-policy-test)#user-role testing precedence 10
rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
  user-role testing precedence 10
  default-role use ip-access-list in test precedence 1
rfs7000-37FABE(config-role-policy-test)#
```

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#?
Role Mode commands:
ap-location          AP Location configuration
assign               Assign parameters to the role
authentication-type  Type of Authentication
captive-portal       Captive-portal based Role Filter
city                 City configuration
client-identity      Client identity
company              Company configuration
country              Country configuration
department           Department configuration
emailid              Emailid configuration
employee-type        Employee-type configuration
employeeld           Employeeid configuration
encryption-type      Type of encryption
group                Group configuration
memberOf             MemberOf configuration
mu-mac               MU MAC address configuration
no                   Negate a command or set its defaults
radius-user          Radius-user configuration
ssid                 SSID configuration
state                State configuration
title                Title configuration
use                  Set setting to use
user-defined         User-defined configuration
clrsr                Clears the display screen
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

| no       | Removes an existing user role |
### 18.1.7.2 user-role commands

#### user-role

The following table summarizes user role configuration mode commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-location</td>
<td>Configures an AP deployment location based filter</td>
<td>page 18-16</td>
</tr>
<tr>
<td>assign</td>
<td>Configures upstream/downstream rate limits and VLAN ID assigned to clients matching the filters defined in the user-defined role</td>
<td>page 18-17</td>
</tr>
<tr>
<td>authentication-type</td>
<td>Configures an authentication type based filter</td>
<td>page 18-19</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures a captive portal based filter</td>
<td>page 18-21</td>
</tr>
<tr>
<td>city</td>
<td>Configures a city name based filter</td>
<td>page 18-22</td>
</tr>
<tr>
<td>client-identity</td>
<td>Associates a client-identity (device fingerprinting) based filter</td>
<td>page 18-23</td>
</tr>
<tr>
<td>company</td>
<td>Configures a company name based filter</td>
<td>page 18-24</td>
</tr>
<tr>
<td>country</td>
<td>Configures a country name based filter</td>
<td>page 18-25</td>
</tr>
<tr>
<td>department</td>
<td>Configures a department name based filter</td>
<td>page 18-26</td>
</tr>
<tr>
<td>emailid</td>
<td>Configures an email ID based filter</td>
<td>page 18-28</td>
</tr>
<tr>
<td>employee-type</td>
<td>Configures an employee type ID based filter</td>
<td>page 18-30</td>
</tr>
<tr>
<td>employeeid</td>
<td>Configures an employee ID based filter</td>
<td>page 18-31</td>
</tr>
<tr>
<td>encryption-type</td>
<td>Configures an encryption type filter</td>
<td>page 18-33</td>
</tr>
<tr>
<td>group</td>
<td>Configures a RADIUS group based filter</td>
<td>page 18-35</td>
</tr>
<tr>
<td>memberOf</td>
<td>Assigns an Active Directory (AD) group to this user-defined role</td>
<td>page 18-37</td>
</tr>
<tr>
<td>mu-mac</td>
<td>Configures MAC address and mask based filter</td>
<td>page 18-38</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets the filters configured on this user-defined role</td>
<td>page 18-39</td>
</tr>
<tr>
<td>radius-user</td>
<td>Configures a wireless client filter based on the RADIUS user name</td>
<td>page 18-41</td>
</tr>
<tr>
<td>ssid</td>
<td>Configures a SSID based filter</td>
<td>page 18-43</td>
</tr>
<tr>
<td>state</td>
<td>Configures a user role state to match</td>
<td>page 18-45</td>
</tr>
<tr>
<td>title</td>
<td>Configures a ‘title’ string to match</td>
<td>page 18-47</td>
</tr>
<tr>
<td>use</td>
<td>Associates a IP and/or MAC ACL with this role. These ACLs specify the action taken when a client matches this user-defined role.</td>
<td>page 18-48</td>
</tr>
<tr>
<td>user-defined</td>
<td>Defines a filter based on an attribute defined in the Active Directory or the OpenLDAP server</td>
<td>page 18-51</td>
</tr>
</tbody>
</table>
18.1.7.2.1 ap-location

- **user-role commands**

Configures an AP's deployment location based filter for this user-defined role

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ap-location [any|contains|exact|not-contains]

ap-location any

ap-location [contains|exact|not-contains] <WORD>

**Parameters**

- **ap-location any**
  - Specifies the AP location to match (in a RF Domain) or the AP's resident configuration
  - any – Defines an AP's location as any

- **ap-location [contains|exact|not-contains] <WORD>**
  - Specifies the AP location to match (in a RF Domain) or the AP's resident configuration. Select one of the following filter options: contains, exact, or not-contains.
  - contains <WORD> – Applies role if the associating AP's location contains the location string specified in the role.
  - exact <WORD> – Applies role if the associating AP's location exactly matches the string specified in the role.
  - not-contains <WORD> – Applies role if the associating AP's location does not contain the location string specified in the role.

**Examples**

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#ap-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
    user-role testing precedence 10
    ap-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

**Related Commands**

- **no** – Removes an AP's deployment location string from this user-defined role
18.1.7.2.2 assign

user-role commands

Configures upstream/downstream rate limits and VLAN ID. Clients matching this user-defined role filters are associated with the specified VLAN, and assigned the specified data rates.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

assign [rate-limit|VLAN]

assign rate-limit [from-client|to-client] <1-65536>
assign vlan <1-4094>

Parameters

- assign rate-limit [from-client|to-client] <1-65536>
- assign vlan <1-4094>

assign rate-limit [from-client|to-client] <1-65536>

Assigns an upstream and downstream traffic rate limit

- from-client – Assigns a rate limit, in Kbps, for the upstream (from client) traffic
- to-client – Assigns a rate limit, in Kbps, for the downstream (to client) traffic
- <1-65536> – Specify upstream and/or downstream rate limits from 1 - 65536 Kbps.

Note: Wireless clients matching this user-defined role are assigned the configured rate limits.

assign vlan <1-4094>

Assigns a VLAN (identified by VLAN’s ID). Clients matching this user-defined role are associated with the specified VLAN. The VLAN ID represents the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). This feature is disabled by default.

- <1-4094> – Specify the VLAN ID from 1 - 4094.

Note: A wireless client that fails to match any user-defined role is assigned to the default role (configured as a role policy setting) and is mapped to the default VLAN under the WLAN.

Usage Guidelines

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

In case of bridge VLAN, the default bridging mode is ‘auto’. Change the bridging mode to ‘tunnel’. This extends the controller’s existing VLAN onto the AP and ensures that wireless clients are served IP addresses.

The VLAN configured under the user-defined role need not exist under the WLAN. But, when using tunneled VLAN bridges, configure an additional bridge VLAN. If the VLAN bridging mode is ‘local’, no additional VLAN configuration is required.
Examples

rfs4000-229D58(config-role-policy-test-user-role-test)#assign rate-limit to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#commit
rfs4000-229D58(config-role-policy-test-user-role-test)#show context
  user-role test precedence 1
  assign vlan 1
  assign rate-limit to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#

The following examples define a role used to forward the IP traffic from all engineers in Test_Company, Santa Clara, USA onto VLAN 2.

1. Create a new role policy with name ‘test-policy’.
   <DEVICE>(config)#role-policy test-policy

2. Specify the LDAP server used for this role policy.
   <DEVICE>(config-role-policy-test-policy)#ldap-query self
   <DEVICE>(config-role-policy-test-policy)#ldap-server 1 host 192.160.1.1 bind-dn
   CN=Administrator,CN=Users,DC=testtest,DC=com base-dn CN=Administrator,CN=Users,DC=com bind-
   password 0 test port 389
   <DEVICE>(config-role-policy-test-policy)#ldap-timeout 2

3. Create a user defined role.
   <DEVICE>(config-role-policy-test-policy)#user-role SCEngineer precedence 100

4. Define the role by adding appropriate values and match operators.
   <DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#city exact santa-clara
   <DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#company exact ExampleCompany
   <DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#country exact usa
   <DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#title contains engineer
   <DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#assign vlan-id 2

5. Apply role policy to an access point.
   ap7131-99BFA8(config-device-ap7131)# use role-policy test-policy

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the upstream and/or downstream rate limits applied to this user-defined role. Also removes the VLAN ID.</td>
</tr>
</tbody>
</table>
18.1.7.2.3 authentication-type

(user-role commands)

Configures the authentication type based filter for this user-defined role.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

\[
\text{authentication-type} \quad \text{[any|eq|neq]} \\
\text{authentication-type} \quad \text{any} \\
\text{authentication-type} \quad \text{[eq|neq]} \quad \text{[eap|kerberos|mac-auth|none]} \\
\quad \{(eap|kerberos|mac-auth|none)\}
\]

Parameters
- authentication-type any


<table>
<thead>
<tr>
<th>any</th>
<th>The authentication type is any (eq or neq). This is the default setting.</th>
</tr>
</thead>
</table>

- authentication-type [eq|neq] [eap|kerberos|mac-auth|none] \{(eap|kerberos|mac-auth|none)\}

<table>
<thead>
<tr>
<th>eq</th>
<th>The role is applied only when the authentication type matches (equals) one or more than one of the following types:</th>
</tr>
</thead>
</table>
| [eap|kerberos|mac-auth|none] | - eap – Extensible authentication protocol  
- kerberos – Kerberos authentication  
- mac-auth – MAC authentication protocol  
- none – no authentication used  
These parameters are recursive, and you can configure more than one unique authentication type for this user-defined role. |

<table>
<thead>
<tr>
<th>neq</th>
<th>The role is applied only when the authentication type does not match (not equals) any of the following types:</th>
</tr>
</thead>
</table>
| [eap|kerberos|mac-auth|none] | - eap – Extensible authentication protocol  
- kerberos – Kerberos authentication  
- mac-auth – MAC authentication protocol  
- none – no authentication used  
These parameters are recursive, and you can configure more than one unique ‘not equal to’ authentication type for this user-defined role. |
Examples

rfs7000-37FABE(config-role-policy-test-user-role-testing)#authentication-type eq kerberos

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
  user-role testing precedence 10
    authentication-type eq kerberos
    ap-location contains office
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the authentication type filter configured for this user-defined role</td>
</tr>
</tbody>
</table>
18.1.7.2.4 captive-portal

user-role commands

Configures a captive portal based filter for this user-defined role. A captive portal is a guest access policy that provides temporary and restrictive access to the wireless network. When applied to a WLAN, a captive portal policy ensures secure guest access.

This command defines user-defined role filters based on a wireless client’s state of authentication.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

captive-portal authentication-state [any|post-login|pre-login]

Parameters
- captive-portal authentication-state [any|post-login|pre-login]

<table>
<thead>
<tr>
<th>authentication-state</th>
<th>Defines the authentication state of a client connecting to a captive portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Specifies any authentication state (authenticated and pending authentication). This is the default setting. This option makes no distinction on whether authentication is conducted before or after the wireless client has logged in.</td>
</tr>
<tr>
<td>post-login</td>
<td>Specifies authentication is completed successfully This option requires the wireless client to share authentication credentials after logging into the managed network.</td>
</tr>
<tr>
<td>pre-login</td>
<td>Specifies authentication is pending This option enables captive portal client authentication before the client is logged into the controller.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-role-policy-test-user-role-testing)#captive-portal authentication-state pre-login
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context user-role testing precedence 10 authentication-type eq kerberos ap-location contains office captive-portal authentication-state pre-login
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

no | Removes the captive portal based role filter settings |
18.1.7.2.5 city

*user-role commands*

Configures a wireless client filter based on the city name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

city [any|contains|exact|not-contains]
city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

**Parameters**
- city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

<table>
<thead>
<tr>
<th>city</th>
<th>Specifies a wireless client filter based on how the 'city' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>No specific city associated with this user-defined role. This role can be applied to any wireless client from any city.</td>
</tr>
</tbody>
</table>
| contains <WORD> | The role is applied only when the city name, returned by the RADIUS server, contains the string specified in the role.  
  - <WORD> – Specify the string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should contain the provided expression. |
| exact | The role is applied only when the city name, returned by the RADIUS server, exactly matches the string specified in the role.  
  - <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should be an exact match. |
| not-contains <WORD> | The role is applied only when the city name, returned by the RADIUS server, does not contain the string specified in the role.  
  - <WORD> – Specify the string not to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should not contain the provided expression. |

**Examples**

rfs7000-37FABE(config-role-policy-test-user-role-testing)#city exact SanJose

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
city exact SanJose
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

**Related Commands**

| no | Removes the city name configured with this user-defined role |
18.1.7.2.6 client-identity

**user-role commands**

Associates a client-identity (device fingerprinting) based filter. The role is assigned to a wireless client matching any of the defined client identities.

For more information on configuring client identity fingerprints, see `client-identity`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

**Parameters**

- `client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}`

<table>
<thead>
<tr>
<th>client-identity <code>&lt;CLIENT-IDENTITY-NAME&gt;</code></th>
<th>Specifies the client-identity fingerprint to match (should be existing and configured)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CLIENT-IDENTITY-NAME&gt;</code></td>
<td>- <code>&lt;CLIENT-IDENTITY-NAME&gt;</code> – Specify the client identity signature name.</td>
</tr>
<tr>
<td><strong>Note:</strong> Multiple client identities can be configured with a role policy.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When associating a single or multiple client identities with a role policy, ensure that in a client identity group, all the client identities used by the role policy, is attached to the device or profile using the role policy. In other words, group all the client identities (used in this role policy) in a client identity group, and associate this group to the profile or device using this role policy.

For more information on configuring client identities and client identity groups, see `client-identity`, and `client-identity-group`.

For more information on associating a client identity group and a role policy to a profile or a device, see `use`.

**Examples**

```
rfs4000-229D58 (config-role-policy-test-user-role-test)#client-identity TestClientIdentity
rfs4000-229D58 (config-role-policy-test-user-role-test)#commit
```

```
rfs4000-229D58 (config-role-policy-test-user-role-test)#client-identity ClientIdentityWindows
rfs4000-229D58 (config-role-policy-test-user-role-test)#
```

```
rfs4000-229D58 (config-role-policy-test-user-role-test)#show context
   user-role test precedence 1
   client-identity TestClientIdentity
   client-identity ClientIdentityWindows
rfs4000-229D58 (config-role-policy-test-user-role-test)#
```

**Related Commands**

| `no` | Removes the client identities associated with this role policy |
18.1.7.2.7 company

▶ user-role commands

Configures a wireless client filter based on the company name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
company [any|contains|exact|not-contains]
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

Parameters
- company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

| company | Specifies a wireless client filter based on how the ‘company’ name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains |
| any | No specific company associated with this user-defined role. This role is applied to any wireless client from any company (no strings to match). This is the default setting. |
| contains <WORD> | The role is applied only when the company name, returned by the RADIUS server, contains the string specified in the role.  
  - <WORD> – Specify the string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should contain the provided expression. |
| exact | The role is applied only when the company name, returned by the RADIUS server, exactly matches the string specified in the role.  
  - <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should be an exact match. |
| not-contains <WORD> | The role is applied only when the company name, returned by the RADIUS server, does not contain the string specified in the role.  
  - <WORD> – Specify the string not to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should not contain the provided expression. |

Examples
rfs7000-37FABE(config-role-policy-test-user-role-testing)#company exact ExampleCompany
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands
no | Removes the company name configured with this user-defined role |
18.1.7.2.8 country

user-role commands

Configures a wireless client filter based on the country name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

country [any|contains|exact|not-contains]
country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

Parameters

- country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

<table>
<thead>
<tr>
<th>country</th>
<th>Specifies a wireless client filter based on how the ‘country’ name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>No specific country associated with this user-defined role. This role is applied to any wireless client from any country (no strings to match). This is the default setting.</td>
</tr>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The role is applied only when the country name, returned by the RADIUS server, contains the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should contain the provided expression.</td>
</tr>
<tr>
<td>exact</td>
<td>The role is applied only when the country name, returned by the RADIUS server, exactly matches the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should be an exact match.</td>
</tr>
<tr>
<td>not-contains &lt;WORD&gt;</td>
<td>The role is applied only when the country name, returned by the RADIUS server, does not contain the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should not contain the provided expression.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-role-policy-test-user-role-testing)#country exact America

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact Examplecompany
  country exact America
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

no | Removes the country name configured with this user-defined role |
18.1.7.2.9 department

*user-role commands*

Configures a wireless client filter based on the department name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

department [any|contains|exact|not-contains]
department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

**Parameters**
- department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

| department | Specifies a wireless client filter based on how the 'department' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains |
| any | No specific department associated with this user-defined role. This role can be applied to any wireless client from any department (no strings to match). This is the default setting. |
| contains <WORD> | The role is applied only when the department name, returned by the RADIUS server, contains the string specified in the role. |
| exact | The role is applied only when the department name, returned by the RADIUS server, exactly matches the string specified in the role. |
| not-contains <WORD> | The role is applied only when the department name, returned by the RADIUS server, does not contain the string specified in the role. |

**Examples**

rfs7000-37FABE(config-role-policy-test-user-role-testing)#department exact TnV
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
department exact TnV
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the department name configured with this user-defined role</td>
</tr>
</tbody>
</table>
### 18.1.7.2.10 emailid

**user-role commands**

Configures a wireless client filter based on the e-mail ID

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
emailid [any|contains|exact|not-contains]
emailid [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

**Parameters**

- `emailid [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

<table>
<thead>
<tr>
<th>emailid</th>
<th>Specifies a wireless client filter based on how the 'e-mail ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>No specific e-mail ID associated with this user-defined role. This role can be applied to any wireless client having any e-mail ID (no strings to match). This is the default setting.</td>
</tr>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The role is applied only when the e-mail ID, returned by the RADIUS server, contains the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should contain the provided expression.</td>
</tr>
<tr>
<td>exact</td>
<td>The role is applied only when the e-mail ID, returned by the RADIUS server, exactly matches the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should be an exact match.</td>
</tr>
<tr>
<td>not-contains &lt;WORD&gt;</td>
<td>The role is applied only when the e-mail ID, returned by the RADIUS server, does not contain the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should not contain the provided expression.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#emailid exact testing@examplecompany.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
rfs7000-37FABE(config-role-policy-test-user-role-testing)#emailid exact testing@examplecompany.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the e-mail ID configured with this user-defined role</td>
</tr>
</tbody>
</table>
18.1.7.2.11 employee-type

`user-role commands`

Configures a wireless client filter based on the employee type

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
employee-type [any|contains|exact|not-contains]
employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

**Parameters**

- `employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

<table>
<thead>
<tr>
<th>employee-type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>No specific employee type associated with this user-defined role. This role can be applied to any wireless client having any employee type (no strings to match). This is the default setting.</td>
</tr>
</tbody>
</table>
| contains <WORD> | The role is applied only when the employee type, returned by the RADIUS server, contains the string specified in the role.  
| exact          | The role is applied only when the employee type, returned by the RADIUS server, exactly matches the string specified in the role.  
| not-contains <WORD> | The role is applied only when the employee type, returned by the RADIUS server, does not contain the string specified in the role. |

**Examples**

- `rfs4000-229D58(config-role-policy-test-user-role-test1)#employee-type exact consultant`
- `rfs4000-229D58(config-role-policy-test-user-role-user1)#show context user-role user1 precedence 1 employee-type exact consultant`
- `rfs4000-229D58(config-role-policy-test-user-role-user1)#`

**Related Commands**

- `no` Removes the employee type filter configured with this user-defined role
18.1.7.2.12 employeeid

**user-role commands**

Configures a wireless client filter based on the employee ID.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
employeeid [any|contains|exact|not-contains]
employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

**Parameters**
- `employeeid [any|contains|exact|not-contains]`
- `employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>employeeid</code></td>
<td>Specifies a wireless client filter based on how the 'employee ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>No specific employee ID associated with this user-defined role. This role can be applied to any wireless client having any employee ID (no strings to match). This is the default setting.</td>
</tr>
<tr>
<td><code>contains &lt;WORD&gt;</code></td>
<td>The role is applied only when the employee ID, returned by the RADIUS server, contains the string specified in the role.</td>
</tr>
<tr>
<td>- <code>&lt;WORD&gt;</code></td>
<td>Specify the string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should contain the provided expression.</td>
</tr>
<tr>
<td><code>exact</code></td>
<td>The role is applied only when the employee ID, returned by the RADIUS server, exactly matches the string specified in the role.</td>
</tr>
<tr>
<td>- <code>&lt;WORD&gt;</code></td>
<td>Specify the exact string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should be an exact match.</td>
</tr>
<tr>
<td><code>not-contains &lt;WORD&gt;</code></td>
<td>The role is applied only when the employee ID, returned by the RADIUS server, does not contain the string specified in the role.</td>
</tr>
<tr>
<td>- <code>&lt;WORD&gt;</code></td>
<td>Specify the string not to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should not contain the provided expression.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#employeeid contains TnVTest1
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
captive-portal authentication-state pre-login
city exact SanJose
country exact America
dept exact TnV
emailid exact testing@examplecompany.com
employeeid contains TnVTest1
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the employee ID configured with this user-defined role</td>
</tr>
</tbody>
</table>
18.1.7.2.13 encryption-type

**user-role commands**

Selects the encryption type for this user-defined role. Encryption ensures privacy between access points and wireless clients. There are various modes of encrypting communication on a WLAN, such as *Counter-model CBC-MAC Protocol (CCMP)*, *Wired Equivalent Privacy (WEP)*, *keyguard*, *Temporal Key Integrity Protocol (TKIP)* etc.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP86XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`encryption-type [any|eq|neq]`

`encryption-type any`

`encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]`

`{(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)}`

**Parameters**

- **encryption-type any**
  - The encryption type can be any one of the listed options (ccmp|keyguard|tkip|wep128|wep64). This is the default setting.

- **encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]**
  - The role is applied only if the encryption type equals to one of the following options:
    - ccmp — Encryption mode is CCMP
    - keyguard — Encryption mode is keyguard. Keyguard encryption shields the master encryption keys from being discovered.
    - none — No encryption mode specified
    - tkip — Encryption mode is TKIP
    - wep128 — Encryption mode is WEP128
    - wep64 — Encryption mode is WEP64
  - These parameters are recursive, and you can configure more than one encryption type for this user-defined role.

- **encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]**
  - The role is applied only if encryption type is not equal to any of the following options:
    - ccmp — Encryption mode is not equal to CCMP
    - keyguard — Encryption mode is not equal to keyguard
    - none — Encryption mode is not equal to none
    - tkip — Encryption mode is not equal to TKIP
    - wep128 — Encryption mode is not equal to WEP128
    - wep64 — Encryption mode is not equal to WEP64
  - These parameters are recursive, and you can configure more than one ‘not equal to’ encryption type for this user-defined role.
Examples
rfs7000-37FABE(config-role-policy-test-user-role-testing)#encryption-type eq wep128
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
  user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnVTest1
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the encryption type configured for this user-defined role</td>
</tr>
</tbody>
</table>
### 18.1.7.2.14 group

**user-role commands**

Configures a wireless client filter based on the RADIUS group name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
group [any|contains|exact|not-contains]
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]  
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Specifies a wireless client filter based on how the RADIUS group name matches the provided expression. Select one of the following options: any, contains, exact, or not-contains</td>
</tr>
<tr>
<td>any</td>
<td>This user-defined role can fit into any group (no strings to match). This is the default setting.</td>
</tr>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The role is applied only when the RADIUS group name contains the string specified in the role.</td>
</tr>
<tr>
<td>exact &lt;WORD&gt;</td>
<td>The role is applied only when the RADIUS group name exactly matches the string specified in the role.</td>
</tr>
<tr>
<td>not-contains &lt;WORD&gt;</td>
<td>The role is applied only when the RADIUS group name does not contain the string specified in the role.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-role-policy-test-user-role-testing)#group contains testgroup
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact Example_company
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeecd contains TnVTest1
```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the group configured for this user-defined role</td>
</tr>
</tbody>
</table>
18.1.7.2.15 **memberOf**

**user-role commands**

Applies an *Active Directory* (AD) group filter to this user-defined role. A wireless client can be a member of more than one group within the AD database. This command applies a AD group based firewall, which applies a role to a wireless client only if it belongs to the specified AD group.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
memberOf <AD-GROUP-NAME>
```

**Parameters**

- **memberOf <AD-GROUP-NAME>**

<table>
<thead>
<tr>
<th><strong>memberOf &lt;AD-GROUP-NAME&gt;</strong></th>
<th>Applies this user-defined role to a client only if the client belongs to the specified AD group</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;AD-GROUP-NAME&gt;</td>
<td>Specify the AD group name.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-role-policy-test-user-role-test)#memberOf ADTestgroup

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
user-role test precedence 1
  assign vlan 1
  assign rate-limit to-client 200
memberOf ADTestgroup
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

**Related Commands**

```
no
```

Removes the AD group assigned to this user-defined role
18.1.7.2.16 mu-mac

*user-role commands*

Configures a MAC address and mask based filter for this role policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

mu-mac [<MAC>|any]

mu-mac any

mu-mac <MAC> {mask <MAC>}

**Parameters**

- mu-mac any

<table>
<thead>
<tr>
<th>any</th>
<th>Applies role to any wireless client (no MAC address to match). This is the default setting.</th>
</tr>
</thead>
</table>
| <MAC> | Applies role to the wireless client having specified MAC address  
  • <MAC> – Sets the MAC address in the AA-BB-CC-DD-EE-FF format |
| mask <MAC> | Optional. After specifying the client's MAC address, specify the mask in the  
  AA-BB-CC-DD-EE-FF format. The role is applied to the wireless client exactly  
  matching the specified MAC address and MAC mask. |

**Examples**

rfs7000-37FABE(config-role-policy-test-user-role-testing)#mu-mac 11-22-33-44-55-66

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context

user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  location contains office
  mu-mac 11-22-33-44-55-66
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeoid contains TnVTest1

rfs7000-37FABE(config-role-policy-test-user-role-testing)#

**Related Commands**

| no | Removes the MAC address and mask for this user-defined role |
18.1.7.2.17 no

user-role commands

Negates a command or resets configured settings to their default. When used in the config role policy user-defined role mode, the no command removes or resets settings, such as AP location, authentication type, encryption type, captive portal etc.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [ap-location|assign|authentication-type|captive-portal|city|client-identity|company|country|department|emailid|employee-type|employeeid|encryption-type|group|memberOf|mu-mac|radius-user|ssid|state|title|use|user-defined]

no captive-portal authentication-state

no use [application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-list|mac-access-list|url-filter]

no use [ip-access-list|ipv6-access-list|mac-access-list] [in|out] <IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>

no use [application-policy|bonjour-gw-discovery-policy|url-filter]

Parameters
- no <PARAMETERS>

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

The following example shows the Role Policy ‘test’ User Role ‘testing’ configuration before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  mu-mac 11-22-33-44-55-66
  group contains testgroup
captive-portal authentication-state pre-login
city exact SanJose
  company exact ExampleCompany
country exact America
department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnV Test1
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no authentication-type
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no encryption-type
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no group
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no mu-mac
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no ap-location
rfs7000-37FABE(config-role-policy-test-user-role-testing)#no employeeid

The following example shows the Role Policy ‘test’ User Role ‘testing’ configuration after the ‘no’ commands are executed:

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
captive-portal authentication-state pre-login
city exact SanJose
company exact ExampleCompany
country exact America
department exact TnV
emailid exact testing@examplecompany.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
18.1.7.2.18 radius-user

▶ user-role commands

Configures a wireless client filter based on the RADIUS user name

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

radius-user [any|contains|ends-with|exact|not-contains|starts-with]

Parameters

- radius-user [any|contains|ends-with|exact|not-contains|starts-with]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-user</td>
<td>Specifies a wireless client filter based on how the 'radius-user' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.</td>
</tr>
<tr>
<td>any</td>
<td>No specific RADIUS user name associated with this user-defined role. This role can be applied to any wireless client (no strings to match). This is the default setting.</td>
</tr>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The role is applied only when the 'radius-user' name, returned by the RADIUS server, contains the string specified in the role. &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should contain the provided expression. Note: You can use the realm or any sub-string of the user name.</td>
</tr>
<tr>
<td>ends-with &lt;WORD&gt;</td>
<td>Enables role assignment on the basis of the wireless client’s “department” and/or “group” &lt;WORD&gt; – Specify the string (could be department/group code). For example: 1005000002. In this the last three digits represent the department/group code. The remaining digits represent user’s badge number. The role is applied only when the ‘radius-user’ name, returned by the RADIUS server, ends with the string specified here.</td>
</tr>
<tr>
<td>exact &lt;WORD&gt;</td>
<td>The role is applied only when the ‘radius-user’ name, returned by the RADIUS server, exactly matches the string specified in the role. &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the ‘radius-user’ name returned by the RADIUS server). It should be an exact match. Note: Provide the complete user name along with the realm.</td>
</tr>
<tr>
<td>not-contains &lt;WORD&gt;</td>
<td>The role is applied only when the ‘radius-user’ name, returned by the RADIUS server, does not contain the string specified in the role. &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the ‘radius-user’ name returned by the RADIUS server). It should not contain the provided expression.</td>
</tr>
</tbody>
</table>
## Examples

rfs7000-37FABE(config-role-policy-test-user-role-testing)#radius-user contains test.com

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 1
  radius-user contains test.com
  company exact ExampleCompany
  emailid exact testing@examplecompany.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the radius-user filter</td>
</tr>
</tbody>
</table>
18.1.7.2.19 ssid

**user-role commands**

Configures a SSID based filter

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

ssid [any|exact|contains|not-contains]

ssid any

ssid [exact|contains|not-contains] <WORD>

**Parameters**

- ssid any

<table>
<thead>
<tr>
<th>ssid any</th>
<th>Specifies a wireless client filter based on how the SSID is specified in a WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• any – The role is applied to any SSID location. This is the default setting.</td>
</tr>
</tbody>
</table>

- ssid [exact|contains|not-contains] <WORD>

<table>
<thead>
<tr>
<th>ssid</th>
<th>Specifies a wireless client filter based on how the SSID is specified in a WLAN. This options are: contains, exact, or not-contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>exact &lt;WORD&gt;</td>
<td>The role is applied only when the SSID, returned by the RADIUS server, exactly matches the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.</td>
</tr>
</tbody>
</table>

| contains <WORD> | The role is applied only when the SSID, returned by the RADIUS server, contains the string specified in the role. |
|                 | • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN. |

| not-contains <WORD> | The role is applied only when the SSID, returned by the RADIUS server, does not contain the string specified in the role. |
|                    | • <WORD> – Specify the SSID string not to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN. |
Examples

rfs7000-37FABE(config-role-policy-test-user-role-testing)#ssid not-contains DevUser

rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context user-role testing precedence 10  ssid not-contains DevUser  captive-portal authentication-state pre-login  city exact SanJose  company exact ExampleCompany  country exact America  department exact TnV  emailid exact testing@examplecompany.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#[

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the SSID configured for a user-defined role</td>
</tr>
</tbody>
</table>
18.1.7.2.20 state

**user-role commands**

Configures a user role state to match with this user-defined role

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
state [any|contains|exact|not-contains]
state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

**Parameters**

- `state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

<table>
<thead>
<tr>
<th>state</th>
<th>Specifies a wireless client filter option based on how the RADIUS state matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>This user role can fit any wireless client irrespective of the state (no strings to match).</td>
</tr>
</tbody>
</table>
| contains <WORD> | The user role is applied only when the RADIUS state contains the string specified in the role.  
  - `<WORD>` – Specify the string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should contain the provided expression. |
| exact <WORD> | The role is applied only when the RADIUS state exactly matches the string specified in the role.  
  - `<WORD>` – Specify the exact string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should be an exact match. |
| not-contains <WORD> | The role is applied only when the RADIUS state does not contain the string specified in the role.  
  - `<WORD>` – Specify the string not to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should not contain the provided expression. |

**Examples**

```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#state exact active
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
city exact SanJose
  company exact ExampleCompany
country exact America
department exact TnV
department exact TnV
emailid exact testing@examplecompany.com
state exact active
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the ‘state’ filter string associated with a user role</td>
</tr>
</tbody>
</table>
18.1.7.2.21 title

**user-role commands**

Configures a 'title' string to match

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

title [any|contains|exact|not-contains]
title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]

**Parameters**

- title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]

<table>
<thead>
<tr>
<th>title</th>
<th>Specifies a wireless client filter based on how the title string, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>This user role can fit any wireless client irrespective of the title (no strings to match).</td>
</tr>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The user role is applied only when the title string, returned by the RADIUS server, contains the string specified in the role.</td>
</tr>
<tr>
<td>exact &lt;WORD&gt;</td>
<td>The role is applied only when the title string, returned by the RADIUS server, exactly matches the string specified in the role.</td>
</tr>
<tr>
<td>not-contains &lt;WORD&gt;</td>
<td>The role is applied only when the title string, returned by the RADIUS server, does not contain the string specified in the role.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-role-policy-test-user-role-testing)#title any

**Related Commands**

no | Removes the 'title’ filter string configured with a user role
18.1.7.2.22 use

*user-role commands*

Configures an access list based firewall with this user role

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, firewalls are mechanisms both *blocking* and *permitting* data traffic based on inbound and outbound IP and MAC rules.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

use [application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-list|mac-access-list|url-filter]

use bonjour-gw-discovery-policy <POLICY-NAME>

use [ip-access-list|ipv6-access-list] [in|out] <IP/ipv6-ACCESS-LIST-NAME> precedence <1-100>

use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>

use url-filter <URL-FILTER-NAME>

**Parameters**

- **use application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-list|mac-access-list|url-filter** <POLICY-NAME>

  - **application-policy** <POLICY-NAME>
    - Uses an existing Application policy with a user role. When associated, the Application policy enforces application assurance for all users using this role.
    - **<POLICY-NAME>** – Specify the Application policy name (should be existing and configured).
    - **Note:** For more information on Application policy, see `application-policy`.

  - **bonjour-gw-discovery-policy** <POLICY-NAME>
    - Uses an existing Bonjour GW Discovery policy with a user role. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming from this specific user roles.
    - **<POLICY-NAME>** – Specify the Bonjour GW Discovery policy name (should be existing and configured).
    - **Note:** For more information on Bonjour GW Discovery policy, see `bonjour-gw-discovery-policy`.

- **use [ip-access-list|ipv6-access-list] [in|out] <IP/IPv6-ACCESS-LIST-NAME> precedence <1-100>**

  - **ip-access-list [in|out]**
    - Uses an IPv4 or IPv6 ACL with this user role
    - **in** – Applies the rule to incoming packets
    - **out** – Applies the rule to outgoing packets
### <IPv4/IPv6-ACCESS-LIST-NAME>
Specify the IPv4/IPv6 access list name.

### precedence <1-100>
After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first.
- `<1-100>` – Sets a precedence from 1 - 100

### mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>
Uses a MAC access list with this user role
- in – Applies the rule to incoming packets
- out – Applies the rule to outgoing packets

### use url-filter <URL-FILTER-NAME>
Uses an existing URL filter that acts as a Web content filter firewall rule.
- `<POLICY-NAME>` – Specify the URL filter name (should be existing and configured).

### Examples
```
rfs7000-37FABE(config-role-policy-test-user-role-testing)#use ip-access-list in test precedence 9
rfs7000-37FABE(config-role-policy-test-user-role-testing)#show context
  user-role testing precedence 10
  ssid not-contains DevUser
captive-portal authentication-state pre-login
city exact SanJose
country exact America
department exact TnV
emailid exact testing@examplecompany.com
state exact active
use ip-access-list in test precedence 9
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
rfs7000-37FABE(config-role-policy-test-user-role-test2)#show context
  user-role test2 precedence 1
  mu-mac A4-D1-D2-BF-3D-19
use ip-access-list in test precedence 9
rfs7000-37FABE(config-role-policy-test-user-role-test2)#
r```

```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes an IP, MAC access list, or a Bonjour GW Discovery policy from use with a user role</td>
</tr>
</tbody>
</table>
### 18.1.7.2.23 user-defined

**user-role commands**

Enables you to define a filter based on an attribute defined in the Active Directory or the OpenLDAP server.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
user-defined <ATTR-STRING> [any|contains|exact|not-contains]
user-defined <ATTR-STRING> [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

**Parameters**

- `user-defined <ATTR-STRING> [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>user-defined &lt;ATTR-STRING&gt;</code></td>
<td>Specify a filter based on an attribute defined in the AD or OpenLDAP server.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;ATTR-NAME&gt;</code> – Specify the attribute string.</td>
</tr>
<tr>
<td></td>
<td>After specifying the attribute name, specify the match type.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>No specific string to match. This role can be applied to any wireless client.</td>
</tr>
<tr>
<td></td>
<td>This is the default setting.</td>
</tr>
<tr>
<td><code>contains &lt;WORD&gt;</code></td>
<td>The role is applied only when the user-defined attribute value, returned by</td>
</tr>
<tr>
<td></td>
<td>the RADIUS server, contains the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;WORD&gt;</code> – Specify the string to match (this is case sensitive, and is</td>
</tr>
<tr>
<td></td>
<td>compared against the value returned by the RADIUS server). It should contain</td>
</tr>
<tr>
<td></td>
<td>the provided expression.</td>
</tr>
<tr>
<td><code>exact &lt;WORD&gt;</code></td>
<td>The role is applied only when the user-defined attribute value, returned by</td>
</tr>
<tr>
<td></td>
<td>the RADIUS server, exactly matches the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;WORD&gt;</code> – Specify the exact string to match (this is case sensitive, and</td>
</tr>
<tr>
<td></td>
<td>is compared against the value returned by the RADIUS server). It should be</td>
</tr>
<tr>
<td></td>
<td>an exact match.</td>
</tr>
<tr>
<td><code>not-contains &lt;WORD&gt;</code></td>
<td>The role is applied only when the user-defined attribute value, returned by</td>
</tr>
<tr>
<td></td>
<td>the RADIUS server, does not contain the string specified in the role.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;WORD&gt;</code> – Specify the string not to match (this is case sensitive, and is</td>
</tr>
<tr>
<td></td>
<td>compared against the value returned by the RADIUS server). It should not</td>
</tr>
<tr>
<td></td>
<td>contain the provided expression.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs4000-229D58(config-role-policy-test-user-role-user1)#user-defined office-location exact EcoSpace
rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
user-role user1 precedence 1
  employee-type exact consultant
  user-defined office-location exact EcoSpace
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

**Related Commands**

```plaintext
no
```

Removes the user-defined filter configured with this user role.
This chapter summarizes *Self Monitoring at Run Time RF* (Smart RF) management policy commands in the CLI command structure.

A Smart RF management policy defines operating and recovery parameters that can be assigned to groups of access points. A Smart RF policy is designed to scan the network to identify the best channel and transmit power for each access point radio.

A Smart RF policy reduces deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each managed radio. Smart RF policies when applied to specific RF Domains, apply site specific deployment configurations and self-healing values to groups of devices within pre-defined physical RF coverage areas.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through the periodic re-calibration of the network. Re-calibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).

Smart RF also provides self-healing functions by monitoring the network in real-time, and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual re-configuration to resolve.

Smart RF is supported on any RF Domain manager. In standalone environments, an individual wireless controller manages the calibration and monitoring phases. In clustered environments, a single wireless controller is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Keep in mind that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.
• If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
• If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks channels specified in the Smart RF policy.
• If no SMART RF policy is mapped, the radio selects a random channel.

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access point detect radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using the `dfs-rehome` command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

**NOTE:** Perform RF planning to ensure overlapping coverage exists at a deployment site, for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it is a temporary measure. You need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist in trouble shooting.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the Smart RF policy instance, use the following commands:

```
<DEVICE>(config)#smart-rf-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#smart-rf-policy test
```

```
rfs7000-37FABE(config-smart-rf-policy-test)#?
```

**Smart RF Mode commands:**

- `area` Specify channel list/ power for an area
- `assignable-power` Specify the assignable power during power-assignment
- `avoidance-time` Time to avoid a channel once dfs/adaptivity avoidance is necessary
- `channel-list` Select channel list for smart-rf
- `channel-width` Select channel width for smart-rf
- `coverage-hole-recovery` Recover from coverage hole
- `enable` Enable this smart-rf policy
- `group-by` Configure grouping parameters
- `interference-recovery` Recover issues due to excessive noise and interference
- `neighbor-recovery` Recover issues due to faulty neighbor radios
- `no` Negate a command or set its defaults
- `sensitivity` Configure smart-rf sensitivity (Modifies various other smart-rf configuration items)
- `smart-ocs-monitoring` Smart off channel scanning

```
clrscre
```

```
commit
```

```
end
```

```
exit
```

```
help
```

```
revert
```

```
service
```

```
show
```

```
write
```

```
rfs7000-37FABE(config-smart-rf-policy-test)#
```

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

# 19.1 smart-rf-policy

The following table summarizes Smart RF policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Configures the channel list and power for a specified area</td>
<td>page 19-4</td>
</tr>
<tr>
<td>assignable-power</td>
<td>Specifies the power range during power assignment</td>
<td>page 19-5</td>
</tr>
<tr>
<td>avoidance-time</td>
<td>Allows Smart RF-enabled radios to avoid Dynamic Frequency Selection (DFS) and/or adaptivity regulated channels on detection of interference or radar. This command configures the period for which the channel is avoided.</td>
<td>page 19-5</td>
</tr>
<tr>
<td>channel-list</td>
<td>Assigns the channel list for the selected frequency</td>
<td>page 19-8</td>
</tr>
<tr>
<td>channel-width</td>
<td>Selects the channel width for Smart RF configuration</td>
<td>page 19-9</td>
</tr>
<tr>
<td>coverage-hole-recovery</td>
<td>Enables recovery from errors</td>
<td>page 19-11</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a Smart RF policy</td>
<td>page 19-14</td>
</tr>
<tr>
<td>group-by</td>
<td>Configures grouping parameters</td>
<td>page 19-15</td>
</tr>
<tr>
<td>interference-recovery</td>
<td>Recovers issues due to excessive noise and interference</td>
<td>page 19-16</td>
</tr>
<tr>
<td>neighbor-recovery</td>
<td>Enables recovery from errors due to faulty neighbor radios</td>
<td>page 19-18</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 19-20</td>
</tr>
<tr>
<td>sensitivity</td>
<td>Configures Smart RF sensitivity</td>
<td>page 19-22</td>
</tr>
<tr>
<td>smart-ocs-monitoring</td>
<td>Applies smart off-channel scanning instead of dedicated detectors</td>
<td>page 19-23</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
19.1.1 area

smart-rf-policy

Configures the channel list and power for a specified area

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

area <AREA-NAME> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>

Parameters

- area <AREA-NAME> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>

Examples

rfs7000-37FABE(config-smart-rf-policy-test)#area test channel-list 2.4GHz 1,2,3

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
rfs7000-37FABE(config-smart-rf-policy-test)#

Related Commands

- no
  Removes channel list/power configuration for an area
### 19.1.2 assignable-power

*smart-rf-policy*

Configures the Smart RF power settings over both 2.4 GHZ and 5.0 GHZ radios

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
assignable-power [2.4GHz|5GHz] [max|min] <1-20>
```

**Parameters**

- `assignable-power [2.4GHz|5GHz] [max|min] <1-20>`

**Examples**

```plaintext
rfs7000-37FABE(config-smart-rf-policy-test)#assignable-power 5GHz max 20
rfs7000-37FABE(config-smart-rf-policy-test)#assignable-power 5GHz min 8
rfs7000-37FABE(config-smart-rf-policy-test)#show context smart-rf-policy test
area test channel-list 2.4GHz 1,2,3
    assignable-power 5GHz min 8
    assignable-power 5GHz max 20
rfs7000-37FABE(config-smart-rf-policy-test)#
```

**Related Commands**

- `no`
  - Resets assignable power to its default
19.1.3 avoidance-time

smart-rf-policy

Allows Smart-RF enabled radios to avoid channels with high levels of interference and channels where radar has been detected.

This command configures the interval for which a channel is avoided on detection of interference or radar, and is applicable only if the channel selection mode is set to Smart and a Smart-RF policy is applied to the access point’s RF Domain. For more information on configuring a radio’s channel of operation, see channel.

Certain 5.0 GHz channels are subject to FCC / ETSI DFS regulations that require channels transmitting critical radar signals to be free of interference from radio signals. Consequently, DFS-enabled 5.0 GHz radios scan and switch channels if radar is detected on their current channel of operation. If radar-free channels are not available, the radio stops transmitting until it identifies a radar-free channel.

Adaptivity is a new European Union (EU) stipulation that requires access points to monitor interference levels on their current channel of operation, and stop functioning on channels with interference levels exceeding ETSI-specified threshold values. When enabled, this feature ensures recovery by switching the radio to a new channel with less interference.

Once adaptivity or DFS is triggered, the radio’s channel is switched based on the channel selection mode specified. If the channel is fixed, the radio attempts to come back to its specified channel of operation after the DFS/adaptivity channel evacuation period has expired.

**NOTE:** To optionally disable the radio from switching back to its original channel of operation, execute the no > dfs-rehome command in the radio interface configuration mode of the access point’s profile or device. For more information, see dfs-rehome.

**NOTE:** For radio’s having channel selection mode set to ACS, Random, or Fixed adaptivity timeout can be configured in the access point’s radio interface mode. For more information, see adaptivity.

On the other hand, if the radio’s channel selection mode is set to Smart or ACS, once adaptivity or DFS is triggered, the channel is avoided until the avoidance-time, specified here, expires. Once the evacuation period has expired, the channel is free for use by both Smart-RF and ACS.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
avoidance-time [adaptivity|dfs] <30-3600>
```

**Parameters**

- avoidance-time [adaptivity|dfs] <30-3600>

| avoidance-time [adaptivity|dfs] | Configures the time for which a channel is avoided after dfs or adaptivity is triggered |
|---------------------------------|---------------------------------------------------------------------------------------|
|                                 | • adaptivity – Sets the time, in minutes, for which a radio avoids an adaptivity-regulated channel detected with interference |
|                                 | • dfs – Sets the time, in minutes, for which a radio avoids a DFS-regulated channel detected with radar |
|                                 | • <30-3600> – Specify a value from 30 - 3600 minutes. The default for both parameters is 90 minutes. |
Examples

nx4500-5CFA2B(config-smart-rf-policy-test)#avoidance-time adaptivity 200

nx4500-5CFA2B(config-smart-rf-policy-test)#avoidance-time dfs 300

nx4500-5CFA2B(config-smart-rf-policy-test)#show context smart-rf-policy test
  avoidance-time dfs 300
  avoidance-time adaptivity 200
nx4500-5CFA2B(config-smart-rf-policy-test)#

nx4500-5CFA2B(config-smart-rf-policy-test)#no avoidance-time adaptivity

nx4500-5CFA2B(config-smart-rf-policy-test)#show context include-factory | include avoidance-time
  avoidance-time dfs 300
  avoidance-time adaptivity 90
nx4500-5CFA2B(config-smart-rf-policy-test)#

Related Commands

| no | Reverts the DFS/adaptivity regulated channel avoidance time to default (90 minutes) |
19.1.4 channel-list

Assigns a list of channels, for the selected frequency, used in Smart RF scans

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

channel-list [2.4GHz|5GHz] <WORD>

Parameters

- channel-list [2.4GHz|5GHz] <WORD>

<table>
<thead>
<tr>
<th>2.4GHz &lt;WORD&gt;</th>
<th>Assigns a channel list for the 2.4 GHz band</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify a comma separated list of channels</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5GHz &lt;WORD&gt;</th>
<th>Assigns a channel list for the 5.0 GHz band</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify a comma separated list of channels</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-smart-rf-policy-test)#channel-list 2.4GHz 1,12
rfs7000-37FABE(config-smart-rf-policy-test)#show context
area test channel-list 2.4GHz 1,2,3
assignable-power 5GHz min 8
assignable-power 5GHz max 20
channel-list 2.4GHz 1,12
rfs7000-37FABE(config-smart-rf-policy-test)#

Related Commands

no

Removes the channel list for the selected frequency
19.1.5 channel-width

smart-rf-policy

Selects the channel width for Smart RF configuration

NOTE: In addition to 20 MHz and 40 MHz, AP82XX also provides support for 80 MHz channels.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

channel-width [2.4GHz|5GHz]

channel-width 2.4GHz [20MHz|40MHz|80MHz|auto]
channel-width 5GHz [20MHz|40MHz|80MHz|auto]

Parameters

- channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]

| 2.4GHz [20MHz|40MHz|80MHz|auto] | Assigns the channel width for the 2.4 GHz band |
|-----------------------------------|---------------------------------------------|
| 20MHz – Assigns the 20 MHz channel width. This is the default setting. |
| 40MHz – Assigns the 40 MHz channel width |
| 80MHz – Assigns the 80 MHz channel width (supported only on AP8232) |
| auto – Assigns the best possible channel in the 20 MHz or 40 MHz channel width |

| 5GHz [20MHz|40MHz|80MHz|auto] | Assigns the channel width for the 5.0 GHz band |
|-----------------------------------|---------------------------------------------|
| 20MHz – Assigns the 20 MHz channel width |
| 40MHz – Assigns the 40 MHz channel width. This is the default setting. |
| 80MHz – Assigns the 80 MHz channel width (supported only on AP8232) |
| auto – Assigns the best possible channel in the 20 MHz, 40 MHz, or 80 MHz channel width |

Usage Guidelines

The 20/40 MHz operation allows the access point to receive packets from clients using 20 MHz, and transmit using 40 MHz. This mode is supported for 11n users on both the 2.4 GHz and 5.0 GHz radios. If an 11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select Automatic to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources.
Examples
rfs7000-37FABE(config-smart-rf-policy-test)#channel-width 5GHz auto

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
  assignable-power 5GHz min 8
  assignable-power 5GHz max 20
  channel-list 2.4GHz 1,12
  channel-width 5GHz auto
rfs7000-37FABE(config-smart-rf-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Resets channel width for the selected frequency to its default</td>
</tr>
</tbody>
</table>
19.1.6 coverage-hole-recovery

Enables recovery from coverage hole errors detected by Smart RF. Use this command to configure the coverage hole recovery settings.

When coverage hole recovery is enabled, on detection of a coverage hole, Smart RF first determines the power increase needed based on the *signal-to-noise ratio* (SNR) for a client as seen by the access point radio. If a client’s SNR is above the specified threshold, the transmit power is increased until the SNR falls below the threshold.

**NOTE:** The coverage-hole-recovery parameters can be modified only if the sensitivity level is set to ‘custom’. For more information see, *sensitivity*.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

coverage-hole-recovery {client-threshold|coverage-interval|interval|snr-threshold}

coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}

coverage-hole-recovery {coverage-interval|interval} [2.4GHz|5GHz] <1-120>

coverage-hole-recovery {snr-threshold [2.4GHz|5GHz] <1-75>}

**Parameters**

- **client-threshold**
  Optional. Specifies the minimum number of clients associated to a radio in order to trigger coverage hole recovery.

  - **2.4GHz <1-255>**
    Specifies the minimum number of clients on the 2.4 GHz band
    - **<1-255>** – Sets a value from 1 - 255. The default is 1.

  - **5GHz <1-255>**
    Specifies the minimum number of clients on the 5.0 GHz band
    - **<1-255>** – Sets a value from 1 - 255. The default is 1.

- **coverage-interval**
  Optional. Specifies the interval between the discovery of a coverage hole and the initiation of coverage hole recovery

  - **2.4GHz <1-120>**
    The following keywords are common to the ‘coverage-interval’ and ‘interval’ parameters:
    - **2.4GHz <1-120>** – Specifies the coverage hole recovery interval on the 2.4 GHz band
    - **<1-120>** – Specify a value from 1 - 120 seconds.

  **Note:** coverage-interval – The default is 10 seconds.

  **Note:** interval – The default is 30 seconds.
### coverage-hole-recovery \{snr-threshold\} [2.4Ghz|5Ghz] <1-75>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5GHz &lt;1-120&gt;</td>
<td>The following keywords are common to the 'coverage-interval' and 'interval' parameters:</td>
</tr>
<tr>
<td></td>
<td>• 5GHz &lt;1-120&gt; – Specifies a coverage hole recovery interval on the 5.0 GHz band</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-120&gt; – Specify a value from 1 - 120 seconds.</td>
</tr>
<tr>
<td></td>
<td>Note: coverage-interval – The default is 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Note: interval – The default is 30 seconds.</td>
</tr>
<tr>
<td>snr-threshold</td>
<td>Optional. Specifies the SNR threshold. This value is the SNR threshold for an associated client as seen by its associated AP radio. When the SNR threshold is exceeded, the radio increases its transmit power to increase coverage for the associated client.</td>
</tr>
<tr>
<td>2.4GHz &lt;1-75&gt;</td>
<td>Specifies SNR threshold on the 2.4 GHz band</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-75&gt; – Sets a value from 1 dB - 75 dB. The default is 20 dB.</td>
</tr>
<tr>
<td>5GHz &lt;1-75&gt;</td>
<td>Specifies SNR threshold on the 5.0 GHz band</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-75&gt; – Sets a value from 1 - 75. The default is 20 dB.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-smart-rf-policy-test)#coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
  sensitivity custom
  assignable-power 5GHz min 8
  assignable-power 5GHz max 20
  channel-list 2.4GHz 1,12
  channel-width 5GHz auto
  coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables recovery from coverage hole errors</td>
</tr>
</tbody>
</table>
19.1.7 dfs

smart-rf-policy

Enables a Smart RF enabled radio to avoid Dynamic Frequency Selection (DFS) regulated channels if radar is detected on those channels. Use this command to configure the period for which a radio avoids the DFS-regulated channel detected with a radar.

Certain 5.0 GHz channels are subject to FCC / ETSI DFS regulations. If a Smart RF enabled radio is on a channel subject to DFS, it switches channels if radar is detected on the assigned 5.0 GHz channel. By default the access point radio attempts to come back to its original channel after the DFS channel evacuation period has expired. To optionally disable the radio from switching back to its original channel of operation, execute the no > dfs-rehome command in the radio interface configuration mode of the access point’s profile.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
dfs avoidance-time <30-3600>

Parameters
- dfs avoidance-time <30-3600>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| dfs avoidance-time <30-3600> | Sets the time, in minutes, for which a radio avoids a DFS-regulated channel detected with a radar.  
|                            | • <30-3600> – Specify a value from 30 - 3600 minutes. The default is 90 minutes. |

Examples
rfs6000-81701D(config-smart-rf-policy-test)#dfs avoidance-time 200
rfs6000-81701D(config-smart-rf-policy-test)#show context
smart-rf-policy test
dfs avoidance-time 200
rfs6000-81701D(config-smart-rf-policy-test)#

Related Commands
- no Reverts the DFS regulated channel avoidance time to default (90 minutes)
**19.1.8 enable**

*smart-rf-policy*

Enables a Smart RF policy

Use this command to enable this Smart RF policy. Once enabled, the policy can be assigned to a RF Domain supporting a network.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
enable
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-smart-rf-policy-test)#enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables a Smart RF policy</td>
</tr>
</tbody>
</table>
19.1.9 group-by

smart-rf-policy

Enables grouping of APs on the basis of their location in a building (floor) or an area.

Within a large RD Domain, grouping of APs (within an area or on the same floor in a building) facilitates statistics gathering and troubleshooting.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
group-by [area|floor]
```

Parameters

```
group-by [area|floor]
```

<table>
<thead>
<tr>
<th>area</th>
<th>Groups radios based on their area of location</th>
</tr>
</thead>
<tbody>
<tr>
<td>floor</td>
<td>Groups radios based on their floor location</td>
</tr>
</tbody>
</table>

**Note:** Both options are disabled by default.

Examples

```
rfs7000-37FABE(config-smart-rf-policy-test)#group-by floor
rfs7000-37FABE(config-smart-rf-policy-test)#show context smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
  group-by floor
  sensitivity custom
  assignable-power 5GHz min 8
  assignable-power 5GHz max 20
  channel-list 2.4GHz 1,12
  channel-width 5GHz auto
  coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

```
no
```

Removes Smart RF group settings.
19.1.10 interference-recovery

Smart RF Policy

Enables interference recovery from neighboring radios and other sources of WiFi and non-WiFi interference. Interference is the excess noise detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interfering sources by monitoring the noise levels and other RF parameters on an access point's current channel. When a noise threshold is exceeded, Smart RF selects an alternative channel with less interference. To avoid channel flapping a hold timer is defined, which disables interference avoidance for a specific period of time upon detection. Interference recovery is enabled by default.

**NOTE:** The interference-recovery parameters can be modified only if the sensitivity level is set to 'custom'. For more information see, *sensitivity*.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
interference-recovery {channel-hold-time|channel-switch-delta|client-threshold|interference|neighbor-offset|noise|noise-factor}
```

```
interference-recovery {channel-switch-delta [2.4GHz|5GHz] <5-35>}
```

```
interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}
```

**Parameters**
- *interference-recovery* {channel-switch-delta [2.4GHz|5GHz] <5-35>}

**channel-switch-delta**

Optional. Configures a threshold value for the difference between interference levels on the current channel and the prospective channel needed to trigger a channel change. If the difference in noise levels on the current channel and the prospective channel is below the configured threshold, the channel is not changed.

* [2.4GHz|5GHz] Selects the band
  - 2.4GHz – Selects the 2.4 GHz band
  - 5GHz – Selects the 5.0 GHz band

* <5-35> Specifies the threshold value for the difference between the current and prospective channel interference levels
  - <5-35> – Sets a value from 5 dBm - 35 dBm. The default setting is 20 dBm for both 2.4 GHz and 5.0 GHz bands.

- *interference-recovery* {channel-hold-time <0-86400>|client-threshold <1-255>|interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}

**channel-hold-time**

Optional. Defines the minimum time between two channel change recoveries

* <0-86400> – Sets the time, in seconds, between channel change assignments based on interference or noise. The default is 7,200 seconds.
Examples
rfs7000-37FABE(config-smart-rf-policy-test)#interference-recovery channel-switch-delta 5GHz 5
rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
group-by floor
sensitivity custom
assignable-power 5GHz min 8
assignable-power 5GHz max 20
channel-list 2.4GHz 1,12
channel-width 5GHz auto
interference-recovery channel-switch-delta 5GHz 5
coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#

Related Commands

no

Disables recovery from excessive noise and interference
19.1.11 neighbor-recovery

smart-rf-policy

Enables recovery from errors due to faulty neighboring radios. Enabling neighbor recovery ensures automatic recovery from failed radios within the radio coverage area. Smart RF instructs neighboring access points to increase their transmit power to compensate for the failed radio. Neighbor recovery is enabled by default when the sensitivity setting is medium.

NOTE: The neighbor-recovery parameters can be modified only if the sensitivity level is set to ‘custom’. For more information see, sensitivity.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

neighbor-recovery {dynamic-sampling|power-hold-time|power-threshold}
neighbor-recovery {dynamic-sampling} {retries <1-10>|threshold <1-30>}
neighbor-recovery {power-hold-time <0-3600>}
neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}

Parameters

- neighbor-recovery {dynamic-sampling} {retries <1-10>|threshold <1-30>}

<table>
<thead>
<tr>
<th>dynamic-sampling</th>
<th>Optional. Enables dynamic sampling on this Smart RF policy. Dynamic sampling allows you to define how Smart RF adjustments are triggered by locking the ‘retry’ and ‘threshold’ values. Dynamic sampling is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries &lt;1-10&gt;</td>
<td>Optional. Specifies the number of retries before allowing a power level adjustments to compensate for a potential coverage hole. • &lt;1-10&gt; – Sets the number of retries from 1 - 10. The default is 3.</td>
</tr>
<tr>
<td>threshold &lt;1-30&gt;</td>
<td>Optional. Specifies the minimum number of sample reports before which a power change requires dynamic sampling • &lt;1-30&gt; – Sets the minimum number of reports from 1 - 30. The default is 5.</td>
</tr>
</tbody>
</table>

- neighbor-recovery {power-hold-time <0-3600>}

<table>
<thead>
<tr>
<th>power-hold-time</th>
<th>Optional. Specifies the minimum time, in seconds, between two power changes on a radio during neighbor-recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-3600&gt;</td>
<td>Sets the time from 0 - 3600 sec. The default is 0 seconds.</td>
</tr>
</tbody>
</table>

- neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}

<table>
<thead>
<tr>
<th>power-threshold</th>
<th>Optional. Specifies the power threshold based on which recovery is performed. The 2.4 GHz/5.0 GHz radio uses the value specified here as the maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within its coverage area.</th>
</tr>
</thead>
</table>
Examples

rfs7000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold 2.4GHz -82
rfs7000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold 5GHz -65
rfs7000-37FABE(config-smart-rf-policy-test)#show context smart-rf-policy test
area test channel-list 2.4GHz 1,2,3
group-by floor
sensitivity custom
assignable-power 5GHz min 8
assignable-power 5GHz max 20
channel-list 2.4GHz 1,12
channel-width 5GHz auto
interference-recovery channel-switch-delta 5GHz 5
neighbor-recovery power-threshold 5GHz -65
neighbor-recovery power-threshold 2.4GHz -82
coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#

Related Commands

| no | Disables recovery from faulty neighbor radios |
19.1.12 no

Negates a command or sets its default. When used in the config Smart RF policy mode, the no command disables or resets Smart RF settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [area|assignable-power|avoidance-time|channel-list|channel-width|coverage-hole-recovery|enable|group-by|interference-recovery|neighbor-recovery|smart-ocs-monitoring]

no area <AREA-NAME> channel-list [2.4GHZ|5GHZ]
no assignable-power [2.4GHZ|5GHZ] [max|min]
no [channel-list|channel-width] [2.4GHZ|5GHZ]
no coverage-hole-recovery [client-threshold|coverage-interval|inteval|snr-threshold] [2.4GHZ|5GHZ]
no avoidance-time [adaptivity|dfs]
no enable
no group-by [area|floor]
no interference-recovery {channel-hold-time|channel-switch-delta [2.4GHZ|5GHZ]} [client-threshold|interference|neighbor-offset|noise|noise-factor]
no neighbor-recovery {dynamic-sampling |retries|threshold|power-hold-time|power-threshold [2.4GHZ|5GHZ]}

Parameters
- no <PARAMETERS>

Examples

The following example shows the Smart RF policy ‘test’ settings before the ‘no’ commands are executed:

```
rf5000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
area test channel-list 2.4GHz 1,2,3
group-by floor
sensitivity custom
assignable-power 5GHz min 8
assignable-power 5GHz max 20
channel-list 2.4GHz 1,12
channel-width 5GHz auto
interference-recovery channel-switch-delta 5GHz 5
neighbor-recovery power-threshold 5GHz -65
neighbor-recovery power-threshold 2.4GHz -82
```
coverage-hole-recovery snr-threshold 5GHz 1
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#no interference-recovery channel-switch-delta 5GHz

rfs7000-37FABE(config-smart-rf-policy-test)#no neighbor-recovery power-threshold 2.4GHz

rfs7000-37FABE(config-smart-rf-policy-test)#no neighbor-recovery power-threshold 5GHz

rfs7000-37FABE(config-smart-rf-policy-test)#no assignable-power 5GHz min

rfs7000-37FABE(config-smart-rf-policy-test)#no assignable-power 5GHz max

The following example shows the Smart RF policy 'test' settings after the 'no' commands are executed:

rfs7000-37FABE(config-smart-rf-policy-test)#show context

smart-rf-policy test
area test channel-list 2.4GHz 1,2,3
group-by floor
sensitivity custom
channel-list 2.4GHz 1,12
channel-width 5GHz auto
coverage-hole-recovery snr-threshold 5GHz 1

rfs7000-37FABE(config-smart-rf-policy-test)#
19.1.13 sensitivity

Configures Smart RF sensitivity level. The sensitivity level determines Smart RF scanning and sampling aggressiveness. For example, a low sensitivity level indicates a less aggressive Smart-RF policy. This translates to fewer samples taken during off-channel scanning and short off-channel durations. When the sensitivity level is set to high, Smart-RF collects more samples, and remains off-channel longer.

The Smart RF sensitivity level options include low, medium, high, and custom. Medium, is the default setting. The custom option allows an administrator to adjust the parameters and thresholds for interference recovery, coverage hole recovery, and neighbor recovery. However, the low, medium, and high settings still allow utilization of these features.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
sensitivity [custom|high|low|medium]
```

Parameters

- sensitivity [custom|high|low|medium]

<table>
<thead>
<tr>
<th>sensitivity</th>
<th>Configures Smart RF sensitivity levels. The options available are: custom, high, low, and medium.</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom</td>
<td>Enables custom interference recovery, coverage hole recovery, and neighbor recovery as additional Smart RF options</td>
</tr>
<tr>
<td>high</td>
<td>High sensitivity</td>
</tr>
<tr>
<td>low</td>
<td>Low sensitivity</td>
</tr>
<tr>
<td>medium</td>
<td>Medium sensitivity. This is the default setting.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To enable the **power** and **channel setting** parameters, set sensitivity to **custom** or **medium**.

To enable the **monitoring** and **scanning** parameters, set sensitivity to **custom**.

To enable the **neighbor recovery, interference and coverage hole recovery** parameters, set sensitivity to **custom**.

Examples

```
rfs7000-37FABE(config-smart-rf-policy-test)#sensitivity high
rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
group-by floor
  sensitivity high
  channel-list 2.4GHz 1,12
  channel-width 5GHz auto
  smart-ocs-monitoring frequency 5GHz 3
  smart-ocs-monitoring frequency 2.4GHz 3
  smart-ocs-monitoring sample-count 5GHz 3
  smart-ocs-monitoring sample-count 2.4GHz 3
  --More--
rfs7000-37FABE(config-smart-rf-policy-test)#
```
19.1.14 smart-ocs-monitoring

Applies smart *Off Channel Scanning* (OCS) instead of dedicated detectors

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
smart-ocs-monitoring {awareness-override|client-aware|extended-scan-frequency|
  frequency|off-channel-duration|power-save-aware|sample-count|voice-aware}
```

```plaintext
smart-ocs-monitoring {awareness-override [schedule|threshold]}
```

```plaintext
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME> <DAY>}
```

```plaintext
smart-ocs-monitoring {awareness-override threshold <10-10000>}
```

```plaintext
smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}
```

```plaintext
smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}
```

```plaintext
smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}
```

```plaintext
smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}
```

```plaintext
smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
```

```plaintext
smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}
```

```plaintext
smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
```

**Parameters**

- **awareness-override**

<table>
<thead>
<tr>
<th>awareness-override</th>
<th>Optional. Use this parameter to configure client awareness settings overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedule &lt;1-3&gt;</td>
<td>Configures a time and day schedule when awareness settings are overridden</td>
</tr>
<tr>
<td>&lt;START-TIME&gt;</td>
<td>• &lt;1-3&gt; – Sets the awareness override schedule index. A maximum of three</td>
</tr>
<tr>
<td>&lt;END-TIME&gt;</td>
<td>• overrides can be configured.</td>
</tr>
<tr>
<td>{&lt;DAY&gt;}</td>
<td>• &lt;START-TIME&gt; – Sets the override start time in HH:MM format</td>
</tr>
<tr>
<td></td>
<td>• &lt;END-TIME&gt; – Sets the override end time in HH:MM format</td>
</tr>
</tbody>
</table>
  |                    | • DAY – Optional. Set the day when the override is active. Use one of the fol-
  |                    | lowing formats: |
  |                    | • all – Override is active on all days |
  |                    | • sun – Override is active only on Sundays |
  |                    | • mon – Override is active only on Mondays |
  |                    | • tue – Override is active only on Tuesdays |
  |                    | • wed – Override is active only on Wednesdays |
  |                    | • thu – Override is active only on Thursdays |
  |                    | • fri – Override is active only on Fridays |
  |                    | • sat – Override is active only on Saturdays |
- **smart-ocs-monitoring** `{awareness-override threshold <10-10000>}`

  **awareness-override threshold <10-10000>**

  Optional. Use this parameter to configure client awareness settings overrides
  - **threshold** – Specifies the threshold after which client awareness settings are overridden. When the specified threshold is reached, awareness settings are overridden.
    - **<10-10000>** – Specify a threshold value from 10 -10000. The default is 10.

- **smart-ocs-monitoring** `{client-aware [2.4GHz|5GHz] <1-255>}`

  **client-aware**

  Optional. Enables client aware scanning on this Smart RF policy
  Use this parameter to configure a client threshold number. When the number of clients connected to a radio equals this threshold number, the radio avoids channel scanning.
  This feature is disabled by default.

  - **2.4GHz <1-255>**
    Enables client aware scanning on the 2.4 GHz band
    Avoids radio scanning when a specified minimum number of clients are present
    - **<1-255>** – Sets the minimum number of clients from 1 - 255. The default is 1 client.

  - **5GHz <1-255>**
    Enables client aware scanning on the 5.0 GHz band
    Avoids radio scanning when a specified minimum number of clients are present
    - **<1-255>** – Sets the minimum number of clients from 1 - 255. The default is 1 client.

- **smart-ocs-monitoring** `{extended-scan-frequency [2.4GHz|5GHz] <0-50>}`

  **extended-scan-frequency**

  Optional. Enables an extended scan, as opposed to a neighbor only scan, on this Smart RF policy. This is the frequency radios use to scan for non-peer radios.

  - **2.4GHz <0-50>**
    Enables extended scan on the 2.4 GHz band
    - **<0-50>** – Sets the number of trails from 0 - 50. The default is 5.

  - **5GHz <0-50>**
    Enables extended scan on the 5.0 GHz band
    - **<0-50>** – Sets the number of trails from 0 - 50. The default is 5.

- **smart-ocs-monitoring** `{frequency [2.4GHz|5GHz] <1-120>}`

  **frequency**

  Optional. Specifies the scan frequency. This is the frequency, in seconds, in which smart-ocs-monitoring changes channels for an off channel scan.

  - **2.4GHz <1-120>**
    Selects the 2.4 GHz band
    - **<1-120>** – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.

  - **5GHz <1-120>**
    Selects the 5.0 GHz band
    - **<1-120>** – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.

- **smart-ocs-monitoring** `{off-channel-duration [2.4GHz|5GHz] <20-150>}`

  **off-channel-duration**

  Optional. Specifies the duration to scan off channel
  This is the duration access point radios use to monitor devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within a RF Domain.

  - **2.4GHz <20-150>**
    Selects the 2.4 GHz band (in milliseconds)
    - **<20-150>** – Sets the off channel duration from 20 - 150 msec. The default is 50 milliseconds.
| **smart-ocs-monitoring** | Optional. Enables power save awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. This setting allows Smart RF to detect power save clients and take them into consideration when performing off channel scans. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio. |
| **power-save-aware** | Optional. Enables power save awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. This setting allows Smart RF to detect power save clients and take them into consideration when performing off channel scans. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio. |
| **sample-count** | Optional. Specifies the number of samples to collect before reporting an issue to the Smart RF master. |
| **voice-aware** | Optional. Enables voice awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio. |

**5GHz <20-150>**

Selects the 5.0 GHz band (in milliseconds)
- `<20-150>` – Sets the off channel duration from 20 - 150 msec. The default is 50 milliseconds.

**2.4GHz [disable|dynamic|strict]**

Sets power save awareness scanning mode on the 2.4 GHz band
- `disable` – Disables power save awareness scanning
- `dynamic` – Dynamically avoids scanning based on traffic for power save (PSP) clients
- `strict` – Strictly avoids scanning when PSP clients are present

**5GHz [disable|dynamic|strict]**

Sets power save awareness scanning mode on the 5.0 GHz band
- `disable` – Disables power save awareness scanning
- `dynamic` – Dynamically avoids scanning based on traffic for PSP clients
- `strict` – Strictly avoids scanning when PSP clients are present

**Note:** The default is dynamic.

**sample-count**

Optional. Specifies the number of samples to collect before reporting an issue to the Smart RF master.

**2.4GHz <1-15>**

Selects the 2.4 GHz band
- `<1-15>` – Specifies the number of samples to collect from 1 - 15. The default is 10.

**5GHz <1-15>**

Selects the 5.0 GHz band
- `<1-15>` – Specifies the number of samples to collect from 1 - 15. The default is 5.

**voice-aware**

Optional. Enables voice awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio.

**2.4GHz [disable|dynamic|strict]**

Specifies the scanning mode on the 2.4 GHz band
- `disable` – Disables voice awareness scanning
- `dynamic` – Dynamically avoids scanning based on traffic for voice clients
- `strict` – Strictly avoids scanning when voice clients are present

**Note:** The default is dynamic.
### 5GHz

[disable|dynamic|strict]

<table>
<thead>
<tr>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>5GHz</td>
</tr>
<tr>
<td>**[disable</td>
</tr>
<tr>
<td>Specifies the scanning mode on the 5.0 GHz band</td>
</tr>
<tr>
<td>• disable – Disables voice awareness scanning</td>
</tr>
<tr>
<td>• dynamic – Dynamically avoids scanning based on traffic for voice clients</td>
</tr>
<tr>
<td>• strict – Strictly avoids scanning when voice clients are present.</td>
</tr>
</tbody>
</table>

**Note:** The default is dynamic.

### Examples

```bash
rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring sample-count 2.4GHz 3

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
  area test channel-list 2.4GHz 1,2,3
  group-by floor
  sensitivity custom
  channel-list 2.4GHz 1,12
  channel-width 5GHz auto
  smart-ocs-monitoring off-channel-duration 2.4GHz 25
  smart-ocs-monitoring frequency 5GHz 3
  smart-ocs-monitoring frequency 2.4GHz 3
  smart-ocs-monitoring sample-count 5GHz 3
  **smart-ocs-monitoring sample-count 2.4GHz 3**
  smart-ocs-monitoring extended-scan-frequency 5GHz 0
  smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
  root-recovery root-path-metric-threshold 800
  --More--
rfs7000-37FABE(config-smart-rf-policy-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables off channel monitoring</td>
</tr>
</tbody>
</table>
This chapter summarizes the Wireless Intrusion Protection Systems (WIPS) policy commands in the CLI command structure.

WIPS is an additional measure of security designed to continuously monitor the network for threats and intrusions. Along with wireless VPNs, encryptions, and authentication policies WIPS enhances the security of a WLAN. The WIPS policy enables detection of intrusions and threats that a managed network is likely to encounter. However, the WIPS policy does not include threat mitigation configurations. These intrusions and threats are available within the WIPS policy configuration mode as pre configured, fixed events. Each event consists of a set of frames or anomalies that may be harmful to the managed network. You can enable/disable various aspects of each individual event.

Events are broadly grouped into the following three categories:

- **Excessive/Thresholdable events**: These events detect DOS attacks, like excessive deauths, EAP floods etc. Threshold limits for such events can be configured for mobile units (MU) and radios. Once these threshold limits are exceeded, an event is triggered. Stations triggering an event are usually filtered. You can configure a filter ageout specifying the time for which the station, triggering the event, is filtered. However, the filter ageout only applies when the MU-threshold is exceeded. When radio threshold is reached, the system raises a warning about the same and updates event history with event details.

- **Station/MU anomalies**: These events are triggered when a MU performs suspicious activities that can compromise the security and stability of the managed network. You can configure a filter ageout, similar to the above class of events, to filter the station triggering such events.

- **AP/neighbor anomalies**: These events are triggered when an AP or neighbor sends suspicious frames. The system cannot filter APs or neighbors triggering such events. However, the system warns you about such attacks, allowing you to take further actions against such APs and neighbors.

In addition to event monitoring configuration, the WIPS policy allows you to configure a list of signatures. Unlike events, signatures are not fixed. You are free to define your own signatures based on a specific set of parameters. A signature is a rule, consisting of a set of fields to match and a corresponding set of actions in case of a match. By default, whenever a signature is matched an event log is triggered. This event log is similar to the one triggered upon an event. In addition to an event log, you can also configure other actions. Signatures have all the features supported by events. In fact most events are internally implemented as signatures.

Signature rules are of the following three types:

- **ssid, ssid length rule**: This signature matches a specified SSID or SSID length. It is mandatory to configure the frame type to match for this signature. When configured, only frame types allowed are beacons, probe requests, and probe responses. Example rule: ssid : AirJack and frame type beacon : Signature for AirJack attack.
• payload rule: This signature matches a particular payload at a particular frame offset. You can restrict these matches based on frame type. Example rule: Payload : 0x00601d Offset 3 : Netstumbler

• address-match rule: This signature matches one or more address fields. The address fields supported are BSSID, source-MAC, and destination-MAC. You can also specify frame types to match. The frame types supported are assoc, auth, beacon, data, deauth, disassoc, mgmt, probe-request, and probe-response.

A WIPS policy, once configured, has to be attached to a RF Domain to take effect. Multiple WIPS policies can be configured at the same time, but only one policy can be attached to a given RF Domain at any time.

---

NOTE: To attach a WIPS policy to a RF Domain, in the RF Domain configuration mode, execute the `use > wips-policy <WIPS-POLICY-NAME>` command. For more information, see `use`.

---

NOTE: With this most recent release, AP7522 and AP7532 model Access Points can provide enhanced sensor support. AP7522 and AP7532 sensors can send data from off-channel-scans while in radio-share promiscuous/inline mode, in addition to the on-channel data captured in radio-share mode. ADSP uses the off-channel-scan data (in addition to the on-channel data) to monitor for rogue intrusions and trigger alarms. OTA Termination is triggered from ADSP to the appropriate radio-share AP to initiate termination.

---

NOTE: AP7522 and AP7532 models also support shared part-time scanning using WIPS in WiNG (using off-channel-scans) and no ADSP. WIPS on WiNG was enhanced to add rogue detection/classification (wired side detection based of MAC Address Offset) and over-the-air (OTA) termination for AP7522 and AP7532 deployments.

Use the (config) instance to configure WIPS policy commands. To navigate to the WIPS policy instance, use the following commands:

```bash
<DEVICE>(config)#wips-policy <POLICY-NAME>
```

```bash
rfs7000-37FABE(config)#wips-policy test
rfs7000-37FABE(config-wips-policy-test)#?
```

WIPS Policy Mode commands:

- `ap-detection`: Rogue AP detection
- `enable`: Enable this wips policy
- `event`: Configure an event
- `history-throttle-duration`: Configure the duration for which event duplicates are not stored in history
- `interference-event`: Specify events which will contribute to smart-rf wifi interference calculations
- `no`: Negate a command or set its defaults
- `signature`: Signature to configure
- `use`: Set setting to use
- `clrscr`: Clears the display screen
- `commit`: Commit all changes made in this session
- `do`: Run commands from Exec mode
- `end`: End current mode and change to EXEC mode
- `exit`: End current mode and down to previous mode
- `help`: Description of the interactive help system
- `revert`: Revert changes
- `service`: Service Commands
- `show`: Show running system information
- `write`: Write running configuration to memory or terminal

```bash
rfs7000-37FABE(config-wips-policy-test)#
```
NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
# 20.1 wips-policy

The following table summarizes WIPS policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-detection</td>
<td>Defines the WIPS AP detection configuration</td>
<td>page 20-5</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a WIPS policy</td>
<td>page 20-7</td>
</tr>
<tr>
<td>event</td>
<td>Configures events</td>
<td>page 20-8</td>
</tr>
<tr>
<td>history-throttle-duration</td>
<td>Configures the duration event duplicates are omitted from the event history</td>
<td>page 20-12</td>
</tr>
<tr>
<td>interference-event</td>
<td>Specifies events contributing to the Smart RF WiFi interference calculations</td>
<td>page 20-13</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 20-14</td>
</tr>
<tr>
<td>signature</td>
<td>Configures a WIPS policy signature and enters its configuration mode</td>
<td>page 20-16</td>
</tr>
<tr>
<td>use</td>
<td>Defines a WIPS policy settings</td>
<td>page 20-32</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
### 20.1.1 ap-detection

**wips-policy**

Enables the detection of unauthorized or unsanctioned APs. Unauthorized APs are untrusted access points connected to an access point managed network. These untrusted APs accept wireless client associations. It is important to detect such rogue APs and declare them unauthorized. Rogue AP detection is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

\[
\text{ap-detection \{age-out|air-termination|interferer-threshold|recurring-event-interval|wait-time\}}
\]

\[
\text{ap-detection \{age-out <30-86400>|interferer-threshold <-100--10>|recurring-event-interval <0-10000>|wait-time <10-600>\}}
\]

\[
\text{ap-detection air-termination \{allow-channel-switch|mode [auto|manual]\}}
\]

**Parameters**
- **ap-detection** \{age-out <30-86400>|interferer-threshold <-100--10>|recurring-event-interval <0-10000>|wait-time <10-600>\}
  - Enables detection of unauthorized or unsanctioned APs
  - **age-out <30-86400>**
    - Optional. Configures the unauthorized AP ageout interval. The WIPS policy uses this value to ageout unauthorized APs.
      - <30-86400> – Sets an ageout interval from 30 - 86400 seconds. The default is 5 minutes (300 seconds).
  - **recurring-event-interval <0-10000>**
    - Configures recurring event interval help of unauthorized APs
      - <0-10000> – Configures the recurring interval between 0 - 10000 seconds. The default is 300 seconds.
  - **interferer-threshold <-100--10>**
    - Configures RSSI threshold value to determine if an unsanctioned AP is an interferer or not
      - <-100--10> – Configures the rssi threshold between -100 - -10 dBm. The default is -75 dBm.
  - **wait-time <10-600>**
    - Optional. Configures the wait time before a detected AP is declared as unauthorized and potentially removed
      - <10-600> – Sets a wait time from 10 - 600 seconds. The default is 1 minute (60 seconds).
- **ap-detection air-termination** \{allow-channel-switch|mode [auto|manual]\}
  - Enables air termination of unauthorized APs. This option is disabled by default.
    - allow-channel-switch – Optional. Allows channel switch of unauthorized APs based on the channel mode. This option is disabled by default.
    - mode [auto|manual] – Optional. Select the mode as auto or manual to configure. The default setting is manual.
Examples

```text
rfs7000-37FABE(config-wips-policy-test)#ap-detection wait-time 15
rfs7000-37FABE(config-wips-policy-test)#ap-detection age-out 50

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  ap-detection-age-out 50
  ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#

nx4500-5CFA8E(config-wips-policy-test)#ap-detection recurring-event-interval 10
nx4500-5CFA8E(config-wips-policy-test)#show context
wips-policy test
  ap-detection recurring-event-interval 10
nx4500-5CFA8E(config-wips-policy-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets unauthorized or unsanctioned AP detection settings to default</td>
</tr>
</tbody>
</table>
20.1.2 enable

> wips-policy

Enables this WIPS policy

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX,
  AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530,
  NX9000, NX9500, NX9510, NX9600

Syntax

enable

Parameters

None

Examples

rfs7000-37FABE(config-wips-policy-test)#enable
rfs7000-37FABE(config-wips-policy-test)#

Related Commands

| no | Enables a WIPS policy |
### 20.1.3 event

**wips-policy**

Configures events, filters and threshold values for this WIPS policy. Events are grouped into three categories, AP anomaly, client anomaly, and excessive. WLANs are baselined for matching criteria. Any deviation from this baseline is considered an anomaly and logged as an event.

---

**NOTE:** By default all event monitoring is disabled.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]
```

```
event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
        impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
        unencrypted-wired-leakage|wireless-bridge]
```

```
event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|
        fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|
        identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|
        non-conforming-data|tkip-mic-counter-measures|wellenreiter] {filter-ageout <0-86400>}
```

```
event enable-all-events
```

```
event excessive [80211-replay-check-failure|aggressive-scanning|auth-server-failures|
        decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|
        dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-station|
        {filter-ageout <0-86400>|threshold-client <0-65535>|threshold-radio <0-65535>}
```

**Parameters**

- **event ap-anomaly** [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
  impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
  unencrypted-wired-leakage|wireless-bridge]

  Enables AP anomaly event tracking
  An AP anomaly event refers to suspicious frames sent by neighboring APs. An administrator enables the filtering of each listed event and sets the thresholds for the generation of event notification and filtering.

  - **ad-hoc-violation** Tracks ad-hoc network violations
  - **airjack** Tracks AirJack attacks
  - **ap-ssid-broadcast-in-beacon** Tracks AP SSID broadcasts in beacon events
  - **asleap** Tracks ASLEAP attacks. These attacks break Lightweight Extensible Authentication Protocol (LEAP) passwords
  - **impersonation-attack** Tracks impersonation attacks. These are also referred to as spoofing attacks, where the attacker assumes the address of an authorized device.
null-probe-response  | Tracks null probe response attacks  
transmitting-device-using-invalid-mac | Tracks the transmitting device using an invalid MAC attacks  
unencrypted-wired-leakage | Tracks unencrypted wired leakage  
wireless-bridge | Tracks *wireless bridge* (WDS) frames  


| client-anomaly | Enables client anomaly event tracking  
|---|---
| These are suspicious events performed by wireless clients compromising the security of the network. An administrator can enable or disable filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action applied.  
| dos-broadcast-deauth | Tracks DoS broadcast deauthentication events  
| fuzzing-all-zero-macs | Tracks Fuzzing: All zero MAC addresses observed  
| fuzzing-invalid-frame-type | Tracks Fuzzing: Invalid frame type detected  
| fuzzing-invalid-mgmt-frames | Tracks Fuzzing: Invalid management frame detected  
| fuzzing-invalid-seq-num | Tracks Fuzzing: Invalid sequence number detected  
| identical-src-and-dest-addr | Tracks identical source and destination addresses detection  
| invalid-8021x-frames | Tracks Fuzzing: Invalid 802.1x frames detected  
| netstumbler-generic | Tracks Netstumbler (v3.2.0, 3.2.3, 3.3.0) events  
| non-conforming-data | Tracks non conforming data packets  
| wellenreiter | Tracks Wellenreiter events  
| filter-ageout <0-86400> | The following keywords are common to all of the above client anomaly events:  
  • filter-ageout <0-86400> – Optional. Configures the filter expiration interval in seconds  
  • <0-86400> – Sets the filter ageout interval from 0 - 86400 seconds. The default is 0 seconds.  

**Note:** For each violation define a filter time in seconds, which determines how long the packets (received from an attacking device) are ignored once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed.  
**Note:** The filter ageout value is applicable across the entire RF Domain using this WIPS policy. If an MU is detected performing an attack and is filtered by one of the APs, the information is passed on to all APs and controllers within the RF Domain through the domain manager. Consequently the MU is filtered, for the specified period of time, across all devices.
### event enable-all-events

| enable-all-events | Enables tracking of all intrusion events (client anomaly and excessive events) |


| excessive | Enables the tracking of excessive events. Excessive events are actions performed continuously and repetitively. These events can impact the performance of the controller managed network. DoS attacks come under this category. |

| 80211-replay-check-failure | Tracks 802.11 replay check failure |
| aggressive-scanning | Tracks aggressive scanning events |
| auth-server-failures | Tracks failures reported by authentication servers |
| decryption-failures | Tracks decryption failures |
| dos-assoc-or-auth-flood | Tracks DoS association or authentication floods |
| dos-eapol-start-storm | Tracks DoS EAPOL start storms |
| dos-unicast-deauth-or-disassoc | Tracks DoS dissociation or deauthentication floods |
| eap-flood | Tracks EAP floods |
| eap-nak-flood | Tracks EAP NAK floods |
| frames-from-unassoc-station | Tracks frames from unassociated clients |

| filter-ageout <0-86400> | The following keywords are common to all excessive events: |
| | - filter-ageout <0-86400> – Optional. Configures a filter expiration interval in seconds. It sets the duration for which the client is filtered. The client is added to a ACL as a special entry and frames received from this client are dropped. |
| | - <0-86400> – Sets a filter ageout interval from 0 - 86400 seconds. The default is 0 seconds. |

**Note:** This value is applicable across the RF Domain. If a client is detected performing an attack and is filtered by one of the APs, the information is passed to the domain controller. The domain controller then propagates this information to all APs and wireless controllers in the RF Domain.

| threshold-client <0-65535> | The following keywords are common to all excessive events: |
| | - threshold-client <0-65535> – Optional. Configures a client threshold value after which the filter is triggered and an event is recorded |
| | - <0-65535> – Sets a wireless client threshold value from 0 - 65535 seconds |

| threshold-radio <0-65535> | The following keywords are common to all excessive events: |
| | - threshold-radio <0-65535> – Optional. Configures a radio threshold value after which the filter is triggered and an event is recorded |
| | - <0-65535> – Sets a radio threshold value from 0 - 65535 seconds |
**Examples**

```
rfs7000-37FABE(config-wips-policy-test)#event excessive 80211-replay-check-failure filter-ageout 9 threshold-client 8 threshold-radio 99
rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
  filter-ageout 9
  event client-anomaly wellenreiter filter-ageout 99
  ap-detection-ageout 50
  ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)^
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables WIPS policy events tracking</td>
</tr>
</tbody>
</table>
20.1.4 history-throttle-duration

- wips-policy

Configures the duration event duplicates are omitted from the event history.

The system maintains a history of all events that have occurred, on each device, within a RF Domain. Sometimes
an event occurs for a prolonged period of time and tends to fill up the event history list. In such a scenario, duplicate
information added to the event history list can be throttled for a specified period of time. Once this period is over,
duplicate entries are once again allowed.

Event history statistics are periodically sent to the domain manager, which can be queried to ascertain the general
health of the domain.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX,
  AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530,
  NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
history-throttle-duration <30-86400>
```

Parameters

- history-throttle-duration <30-86400>

Examples

```plaintext
rfs7000-37FABE(config-wips-policy-test)#history-throttle-duration 77
rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  history-throttle-duration 77
  event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
  filter-ageout 9
  event client-anomaly wellenreiter filter-ageout 99
  ap-detection-ageout 50
  ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

Related Commands

```plaintext
no
```

Resets the history throttle duration to its default (120 seconds)
20.1.5 interference-event

wips-policy

Specifies events contributing to the Smart RF WiFi interference calculations

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

interference-event [non-conforming-data|wireless-bridge]

Parameters

- interference-event [non-conforming-data|wireless-bridge]

<table>
<thead>
<tr>
<th>non-conforming-data</th>
<th>Considers non conforming data packets when calculating Smart RF interference</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless-bridge</td>
<td>Considers Wireless Bridge (WDS) frames when calculating Smart RF interference</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-wips-policy-test)#interference-event non-conforming-data

rfs7000-37FABE(config-wips-policy-test)#show context

wips-policy test

history-throttle-duration 77

event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99

filter-ageout 9

event client-anomaly wellenreiter filter-ageout 99

interference-event non-conforming-data

ap-detection-ageout 50

ap-detection-wait-time 15

rfs7000-37FABE(config-wips-policy-test)#

Related Commands

no

Disables this WIPS policy signature as a Smart RF interference source
20.1.6 no

Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the no command negates or resets filters and thresholds.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9600

Syntax

no [ap-detection|enable|event|history-throttle-duration|interference-event|signature|use]

no [enable|history-throttle-duration]

no ap-detection {ageout {[<LINE-SINK>]|air-termination|interferer-threshold <-100--10>|recurring-event-interval <0-10000>wait-time {[<LINE-SINK>]}}

no event [ap-anomaly|client-anomaly|enable-all-events|excessive]


no interference-event [non-conforming-data|wireless-bridge]

no signature <WIPS-SIGNATURE>

no use device-categorization

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the no command negates or resets filters and thresholds. |

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.
Examples
The following example shows the WIPS Policy ‘test’ settings before the ‘no’ commands are executed:
```bash
rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  history-throttle-duration 77
  event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
  filter-ageout 9
  event client-anomaly wellenreiter filter-ageout 99
  interference-event non-conforming-data
  ap-detection-ageout 50
  ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```
```bash
rfs7000-37FABE(config-wips-policy-test)#no event client-anomaly wellenreiter filter-ageout 99
rfs7000-37FABE(config-wips-policy-test)#no interference-event non-conforming-data
rfs7000-37FABE(config-wips-policy-test)#no history-throttle-duration
```

The following example shows the WIPS Policy ‘test’ settings after the ‘no’ commands are executed:
```bash
rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
  filter-ageout 9
  no event client-anomaly wellenreiter filter-ageout 99
  ap-detection-ageout 50
  ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```
20.1.7 signature

* wips-policy

Attack and intrusion patterns are identified and configured as signatures in a WIPS policy. The WIPS policy compares packets in the network with pre configured signatures to identify threats.

The following table summarizes WIPS policy signature configuration commands:

<table>
<thead>
<tr>
<th>Table 20.2 WIPS-Policy-Signature-Config Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>signature</strong></td>
</tr>
<tr>
<td><strong>signature mode commands</strong></td>
</tr>
</tbody>
</table>
20.1.7.1 signature

`signature`

Configures a WIPS policy signature

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`signature <SIGNATURE-NAME>`

Parameters

- `signature <SIGNATURE-NAME>`

Examples

```
rfs7000-37FABE(config-wips-policy-test)#signature test
rfs7000-37FABE(config-test-signature-test)#
```

```
rfs7000-37FABE(config-test-signature-test)#?
Wips Signature Mode commands:
bssid               Bssid mac address
dst-mac             Destination mac address
filter-ageout       Configure filter ageout
frame-type          Configure frame-type to match
interference-event  Signature is a smart-rf interference source
mode                Enable/Disable signature
no                  Negate a command or set its defaults
payload             Configure a payload
src-mac             Source mac address
ssid-match          Match based on ssid
threshold-client    Configure client threshold limit
threshold-radio     Configure radio threshold limit
clrscr              Clears the display screen
commit              Commit all changes made in this session
do                  Run commands from Exec mode
end                  End current mode and change to EXEC mode
exit                 End current mode and down to previous mode
help                 Description of the interactive help system
revert               Revert changes
service              Service Commands
show                 Show running system information
write                Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-test-signature-test)#
```
rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
  filter-ageout 9
  no event client-anomaly wellenreiter filter-ageout 99

  signature test
    interference-event
    bssid 11-22-33-44-55-66
    dst-mac 55-66-77-88-99-00
    frame-type reassoc
    filter-ageout 8
    threshold-client 88
    payload 1 pattern test offset 1
    ap-detection-ageout 50
    ap-detection-wait-time 15

rfs7000-37FABE(config-wips-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Deletes a WIPS policy signature</td>
</tr>
</tbody>
</table>
20.1.7.2 signature mode commands

The following table summarizes WIPS policy signature configuration mode commands:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>bssid</td>
<td>Configures the BSSID MAC address</td>
<td>page 20-20</td>
</tr>
<tr>
<td>dst-mac</td>
<td>Configures the destination MAC address</td>
<td>page 20-21</td>
</tr>
<tr>
<td>filter-ageout</td>
<td>Configures the filter ageout interval</td>
<td>page 20-22</td>
</tr>
<tr>
<td>frame-type</td>
<td>Configures the frame type used for matching</td>
<td>page 20-23</td>
</tr>
<tr>
<td>interference-event</td>
<td>Configures this WIPS policy signature as the Smart RF interference source</td>
<td>page 20-24</td>
</tr>
<tr>
<td>mode</td>
<td>Enables the signature mode</td>
<td>page 20-25</td>
</tr>
<tr>
<td>payload</td>
<td>Configures payload settings</td>
<td>page 20-26</td>
</tr>
<tr>
<td>src-mac</td>
<td>Configures the source MAC address</td>
<td>page 20-27</td>
</tr>
<tr>
<td>ssid-match</td>
<td>Configures a match based on SSID</td>
<td>page 20-28</td>
</tr>
<tr>
<td>threshold-client</td>
<td>Configures the wireless client threshold limit</td>
<td>page 20-29</td>
</tr>
<tr>
<td>threshold-radio</td>
<td>Configures the radio threshold limit</td>
<td>page 20-30</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 20-31</td>
</tr>
</tbody>
</table>
## 20.1.7.2.1 bssid

*signature mode commands*

Configures a BSSID MAC address with this WIPS signature for matching

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`bssid <MAC>`

**Parameters**

- `bssid <MAC>`

<table>
<thead>
<tr>
<th><strong>bssid &lt;MAC&gt;</strong></th>
<th>Configures a BSSID MAC address to match</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;</td>
<td>Specify the MAC address.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-test-signature-test)#bssid 11-22-33-44-55-66
rfs7000-37FABE(config-test-signature-test)#show context signature test
bssid 11-22-33-44-55-66
rfs7000-37FABE(config-test-signature-test)#
```

**Related Commands**

| **no** | Disables a WIPS signature BSSID |
20.1.7.2.2 dst-mac

*signature mode commands*

Configures a destination MAC address for the packet examined for matching

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

dst-mac <MAC>

**Parameters**

- **dst-mac <MAC>**

<table>
<thead>
<tr>
<th>dst-mac &lt;MAC&gt;</th>
<th>Configures a destination MAC address to match</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;</td>
<td>Specify the destination MAC address.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-test-signature-test)#dst-mac 55-66-77-88-99-00

rfs7000-37FABE(config-test-signature-test)#show context signature test

  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00

rfs7000-37FABE(config-test-signature-test)#

**Related Commands**

| no | Disables a WIPS signature destination MAC address |
20.1.7.2.3 filter-ageout

signature mode commands

Configures the filter ageout interval in seconds. This is the duration a client, triggering a WIPS event, is excluded from RF Domain manager radio association.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
filter-ageout <1-86400>

Parameters
- filter-ageout <1-86400>

Examples
rfs7000-37FABE(config-test-signature-test)#filter-ageout 8
rfs7000-37FABE(config-test-signature-test)#show context signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  filter-ageout 8
rfs7000-37FABE(config-test-signature-test)#

Related Commands
- no
  Removes the configured filter ageout interval
20.1.7.2.4 frame-type

*signature mode commands*

Configures the frame type used for matching with this WIPS policy signature

Supported in the following platforms:
  • Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6523, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  • Wireless Controllers — RFS4000, RFS6000, RFS7000
  • Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|reassoc]
```

**Parameters**

- `frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|reassoc]`

<table>
<thead>
<tr>
<th>frame-type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Configures all frame type matching</td>
</tr>
<tr>
<td>assoc</td>
<td>Configures association frame matching</td>
</tr>
<tr>
<td>auth</td>
<td>Configures authentication frame matching</td>
</tr>
<tr>
<td>beacon</td>
<td>Configures beacon frame matching</td>
</tr>
<tr>
<td>data</td>
<td>Configures data frame matching</td>
</tr>
<tr>
<td>deauth</td>
<td>Configures deauthentication frame matching</td>
</tr>
<tr>
<td>disassoc</td>
<td>Configures disassociation frame matching</td>
</tr>
<tr>
<td>mgmt</td>
<td>Configures management frame matching</td>
</tr>
<tr>
<td>probe-req</td>
<td>Configures probe request frame matching</td>
</tr>
<tr>
<td>probe-resp</td>
<td>Configures probe response frame matching</td>
</tr>
<tr>
<td>reassoc</td>
<td>Configures re-association frame matching</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The frame type configured determines the SSID match type configured. To configure the SSID match type as SSID, the frame type must be beacon, probe-req or probe-resp.

**Examples**

```
rfs7000-37FABE(config-test-signature-test)#frame-type reassoc
rfs7000-37FABE(config-test-signature-test)#show context
signature test
  bssid 11-22-33-44-55-66
dst-mac 55-66-77-88-99-00
  frame-type reassoc
filter-ageout &
rfs7000-37FABE(config-test-signature-test)#
```

**Related Commands**

- `no` | Resets a WIPS signature frame type |
20.1.7.2.5 interference-event

\(* signature mode commands \)

Configures this WIPS policy signature as Smart RF interference source

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
interference-event
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-test-signature-test)#interference-event
```

```
rfs7000-37FABE(config-test-signature-test)#show context
signature test
    interference-event
    bssid 11-22-33-44-55-66
    dst-mac 55-66-77-88-99-00
    frame-type reassoc
    filter-ageout 8
rfs7000-37FABE(config-test-signature-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables this WIPS policy signature as Smart RF interference source</td>
</tr>
</tbody>
</table>
20.1.7.2.6 mode

- **signature mode commands**

Enables a WIPS policy signature

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
mode enable
```

**Parameters**

- `mode enable`

<table>
<thead>
<tr>
<th>mode enable</th>
<th>Enables this WIPS signature</th>
</tr>
</thead>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-test-signature-test)#mode enable
rfs7000-37FABE(config-test-signature-test)#
```

**Related Commands**

- `no` Disables a WIPS signature
20.1.7.2.7 payload

*signature mode commands*

Configures payload settings. The payload command sets a numerical index pattern and offset for this WIPS signature.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
payload <1-3> pattern <WORD> offset <0-255>

**Parameters**

<table>
<thead>
<tr>
<th>payload &lt;1-3&gt;</th>
<th>Configures payload settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3&gt;</td>
<td>Sets the payload index from 1 - 3.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pattern &lt;WORD&gt;</th>
<th>Specifies the pattern to match: hex or string</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>Sets the pattern name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>offset &lt;0-255&gt;</th>
<th>Specifies the payload offset to start the pattern match</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-255&gt;</td>
<td>Sets the offset value from 0 - 255</td>
</tr>
</tbody>
</table>

**Examples**

```
> rfs7000-37FABE(config-test-signature-test)#payload 1 pattern test offset 1

> rfs7000-37FABE(config-test-signature-test)#show context
signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type assoc
  filter-ageout 8

> payload 1 pattern test offset 1

> rfs7000-37FABE(config-test-signature-test)#
```
20.1.7.2.8 src-mac

signature mode commands

Configures a source MAC address for a packet examined for matching

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

src-mac <MAC>

Parameters

- src-mac <MAC>

<table>
<thead>
<tr>
<th>src-mac &lt;MAC&gt;</th>
<th>Configures the source MAC address to match</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt; – Specify the source MAC address.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-test-signature-test)#src-mac 00-1E-E5-EA-1D-60

rfs7000-37FABE(config-test-signature-test)#show context signature test
bssid 11-22-33-44-55-66
src-mac 00-1E-E5-EA-1D-60
dst-mac 55-66-77-88-99-00
frame-type assoc
filter-ageout 8
payload 1 pattern test offset 1
rfs7000-37FABE(config-test-signature-test)#

Related Commands

no | Removes a WIPS signature source MAC address
20.1.7.2.9 ssid-match

Configures the SSID (and its character length) used for matching

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ssid-match [ssid|ssid-len]
```

```
ssid-match [ssid <SSID>|ssid-len <0-32>]
```

Parameters

- `ssid-match [ssid <SSID>|ssid-len <0-32>]`

  `ssid <SSID>`

  Specifies the SSID match string
  
  - `<SSID>` — Specify the SSID string.
  
  **Note:** Specify the correct SSID to ensure proper filtering.

  `ssid-len <0-32>`

  Specifies the length of the SSID
  
  - `<0-32>` — Specify the SSID length from 0 - 32 characters.

Examples

```
rfs7000-37FABE(config-test-signature-test)#ssid-match ssid PrinterLan
```

```
rfs7000-37FABE(config-test-signature-test)#show context
signature test
bssid 11-22-33-44-55-66
src-mac 00-1E-E5-EA-1D-60
dst-mac 55-66-77-88-99-00
frame-type beacon
ssid-match ssid PrinterLan
filter-ageout 8
payload 1 pattern test offset 1
rfs7000-37FABE(config-test-signature-test)#
```

Related Commands

```
no
```

Removes the configured SSID
20.1.7.2.10 threshold-client

> **signature mode commands**

Configures the wireless client threshold limit. When the wireless client exceeds the specified limit, an event is triggered.

**Supported in the following platforms:**
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

threshold-client <1-65535>

**Parameters**

- threshold-client <1-65535>

<table>
<thead>
<tr>
<th>threshold-client</th>
<th>Configures the wireless client threshold limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>• &lt;1-65535&gt; – Sets the threshold limit for a 60 second window from 1 - 65535</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-test-signature-test)#threshold-client 88

rfs7000-37FABE(config-test-signature-test)#show context
signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  payload 1 pattern test offset 1
rfs7000-37FABE(config-test-signature-test)#

**Related Commands**

| no | Removes the wireless client threshold limit configured with a WIPS policy signature |
20.1.7.2.11 threshold-radio

`signature mode commands`

Configures the radio’s threshold limit. When the radio exceeds the specified limit, an event is triggered.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510

Syntax

```plaintext
threshold-radio <1-65535>
```

Parameters

- `threshold-radio <1-65535>`

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold-radio &lt;1-65535&gt;</td>
<td>Configures the radio’s threshold limit</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-65535&gt;</code> – Specify the threshold limit for a 60 second window from 1 - 65535.</td>
</tr>
</tbody>
</table>

Examples

```plaintext
rfs7000-37FABE(config-test-signature-test)#threshold-radio 88

rfs7000-37FABE(config-test-signature-test)#show context
signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  threshold-radio 88
  payload 1 pattern test offset 1

rfs7000-37FABE(config-test-signature-test)#
```

Related Commands

```plaintext
no
```

Removes the radio’s threshold limit configured with a WIPS policy signature
20.1.7.2.12 no

signature mode commands

Negates a command or resets settings to their default. When used in the config WIPS policy signature mode, the no command resets or removes WIPS signature settings.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode|payload|src-mac|ssid-match|threshold-client|threshold-radio]

Parameters
- no <PARAMETERS>

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

The following is the WIPS signature ‘test’ settings before the execution of the ‘no’ command:

rfs7000-37FABE(config-test-signature-test)#show context
signature test
bssid 11-22-33-44-55-66
src-mac 00-1E-E5-EA-1D-60
dst-mac 55-66-77-88-99-00
frame-type beacon
ssid-match ssid PrinterLan
filter-ageout 8
threshold-client 88
threshold-radio 88
payload 1 pattern test offset 1
rfs7000-37FABE(config-test-signature-test)#

The following is the WIPS signature ‘test’ settings after the execution of the ‘no’ command:

rfs7000-37FABE(config-test-signature-test)#no mode enable
rfs7000-37FABE(config-test-signature-test)#no bssid
rfs7000-37FABE(config-test-signature-test)#no dst-mac
rfs7000-37FABE(config-test-signature-test)#no src-mac
rfs7000-37FABE(config-test-signature-test)#no filter-ageout
rfs7000-37FABE(config-test-signature-test)#no threshold-client
rfs7000-37FABE(config-test-signature-test)#no threshold-radio
rfs7000-37FABE(config-test-signature-test)#
signature test
no mode enable
frame-type beacon
payload 1 pattern test offset 1
rfs7000-37FABE(config-test-signature-test)
20.1.8 use

wips-policy

Enables device categorization on this WIPS policy. This command uses an existing device categorization list. The list categorizes devices as authorized or unauthorized.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

use device-categorization <DEVICE-CATEGORIZATION>

Parameters

- use device-categorization <DEVICE-CATEGORIZATION>

Examples

rfs7000-37FABE(config-wips-policy-test)#use device-categorization test

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
  filter-ageout 9
  no event client-anomaly wellenreiter filter-ageout 99
  signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
  threshold-client 88
  payload 1 pattern test offset 1
  ap-detection-ageout 50
  ap-detection-wait-time 15
  use device-categorization test
rfs7000-37FABE(config-wips-policy-test)#

Related Commands

- no Disables the use of a device categorization policy with a WIPS policy
CHAPTER 21
WLAN-QOS-POLICY

This chapter summarizes the WLAN QoS policy in the CLI command structure.

A WLAN QoS policy increases network efficiency by prioritizing data traffic. Prioritization reduces congestion. This is essential because of the lack of bandwidth for all users and applications. QoS helps ensure each WLAN on the wireless controller receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as Video, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN.

Each WLAN QoS policy has a set of parameters which it groups into categories, such as management, voice and data. Packets within each category are processed based on the weights defined for each WLAN.

Use the (config) instance to configure WLAN QoS policy commands. To navigate to the WLAN QoS policy instance, use the following commands:

```
<DEVICE>(config)#wlan-qos-policy <POLICY-NAME>
```

```
rfs7000-37FABE(config)#wlan-qos-policy test
rfs7000-37FABE(config-wlan-qos-test)#?
```

**WLAN QoS Mode commands:**
- `accelerated-multicast`: Configure accelerated multicast streams address and forwarding QoS classification
- `classification`: Select how traffic on this WLAN must be classified (relative prioritization on the radio)
- `multicast-mask`: Egress multicast mask (frames that match bypass the PSpQueue. This permits intercom mode operation without delay even in the presence of PSP clients)
- `no`: Negate a command or set its defaults
- `qos`: Quality of service
- `rate-limit`: Configure traffic rate-limiting parameters on a per-wlan/per-client basis
- `svp-prioritization`: Enable spectralink voice protocol support on this wlan
- `voice-prioritization`: Prioritize voice client over other client (for non-WMM clients)
- `wmm`: Configure 802.11e/Wireless MultiMedia parameters
- `clrscr`: Clears the display screen
- `commit`: Commit all changes made in this session
- `do`: Run commands from Exec mode
- `end`: End current mode and change to EXEC mode
- `exit`: End current mode and down to previous mode
- `help`: Description of the interactive help system
- `revert`: Revert changes
- `service`: Service Commands
- `show`: Show running system information
- `write`: Write running configuration to memory or terminal

```
rfs7000-37FABE(config-wlan-qos-test)#
```
NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
21.1 wlan-qos-policy

WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio’s themselves, independent from the wireless clients these access point radios support.

The following table summarizes WLAN QoS policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Configures accelerated multicast stream addresses and forwards QoS classifications</td>
<td>page 21-4</td>
</tr>
<tr>
<td>classification</td>
<td>Classifies WLAN traffic based on priority</td>
<td>page 21-6</td>
</tr>
<tr>
<td>multicast-mask</td>
<td>Configures the egress prioritization multicast mask</td>
<td>page 21-8</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 21-9</td>
</tr>
<tr>
<td>qos</td>
<td>Defines the QoS configuration</td>
<td>page 21-10</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Configures the WLAN traffic rate limit using a WLAN QoS policy</td>
<td>page 21-11</td>
</tr>
<tr>
<td>svp-prioritization</td>
<td>Enables Spectralink voice protocol support on a WLAN</td>
<td>page 21-14</td>
</tr>
<tr>
<td>voice-prioritization</td>
<td>Prioritizes voice client over other clients</td>
<td>page 21-15</td>
</tr>
<tr>
<td>wmm</td>
<td>Configures 802.11e/wireless multimedia parameters</td>
<td>page 21-16</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
21.1.1 accelerated-multicast

`wlan-qos-policy`

Configures the accelerated multicast stream address and forwarding QoS classification settings.

Enabling this option allows the system to automatically detect and convert multicast streams to unicast streams. When a stream is converted and queued up for transmission, there are a number of classification mechanisms that can be applied to the stream. Use the classification options to specify the traffic type to prioritize.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`accelerated-multicast [<IP>|autodetect]`

`accelerated-multicast [<IP>|autodetect] {classification [background|best-effort|trust|video|voice]}

**Parameters**

- `accelerated-multicast [<IP>|autodetect] {classification [background|best-effort|trust|video|voice]}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accelerated-multicast</code></td>
<td>Configures the accelerated multicast stream address and forwarding QoS classification</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Configures a multicast IP address in the A.B.C.D format. The system can configure up to 32 IP addresses for each WLAN QoS policy</td>
</tr>
<tr>
<td><code>autodetect</code></td>
<td>Allows the system to automatically detect multicast streams to be accelerated. This parameter allows the system to convert multicast streams to unicast, or to specify multicast streams converted to unicast.</td>
</tr>
<tr>
<td><code>classification</code></td>
<td>Optional. Configures the QoS classification (traffic class) settings. When the stream is converted and queued for transmission, specify the type of classification applied to the stream. The options are: background, best-effort, trust, voice, and video.</td>
</tr>
<tr>
<td><code>background</code></td>
<td>Forwards streams with background (low) priority. This parameter is common to both <code>&lt;IP&gt;</code> and auto detect.</td>
</tr>
<tr>
<td><code>best-effort</code></td>
<td>Forwards streams with best effort (normal) priority. This parameter is common to both <code>&lt;IP&gt;</code> and autodetect.</td>
</tr>
<tr>
<td><code>trust</code></td>
<td>No change to the streams forwarding traffic class. This parameter is common to both <code>&lt;IP&gt;</code> and autodetect.</td>
</tr>
<tr>
<td><code>video</code></td>
<td>Forwards streams with video traffic priority. This parameter is common to both <code>&lt;IP&gt;</code> and autodetect.</td>
</tr>
<tr>
<td><code>voice</code></td>
<td>Forwards streams with voice traffic priority. This parameter is common to both <code>&lt;IP&gt;</code> and autodetect.</td>
</tr>
</tbody>
</table>
Examples
rfs7000-37FABE(config-wlan-qos-test)#accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#show context wlan-qos-policy test
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
21.1.2 classification

-wlan-qos-policy

Specifies how traffic on this WLAN is classified. This classification is based on relative prioritization on the radio.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

classification [low|non-unicast|non-wmm|normal|video|voice|wmm]
classification [low|normal|video|voice|wmm]
classification non-unicast [voice|video|normal|low|default]
classification non-wmm [voice|video|normal|low]

Parameters

- classification [low|normal|video|voice|wmm]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio</td>
</tr>
<tr>
<td>normal</td>
<td>Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio</td>
</tr>
<tr>
<td>video</td>
<td>Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio</td>
</tr>
<tr>
<td>voice</td>
<td>Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio</td>
</tr>
<tr>
<td>wmm</td>
<td>Uses WMM based classification, using DSCP or 802.1p tags, to classify traffic into different queues Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). The WMM classification supports high throughput data rates required for 802.11n device support. This is the default setting.</td>
</tr>
</tbody>
</table>

- classification non-unicast [voice|video|normal|low|default]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-unicast</td>
<td>Optimized for non-unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multiple destinations</td>
</tr>
<tr>
<td>video</td>
<td>Optimized for non-unicast video traffic. Implies all WLAN non-unicast traffic is classified and treated as video packets</td>
</tr>
<tr>
<td>voice</td>
<td>Optimized for non-unicast voice traffic. Implies all WLAN non-unicast traffic is classified and treated as voice packets</td>
</tr>
<tr>
<td>normal</td>
<td>Optimized for non-unicast best effort traffic. Implies all WLAN non-unicast traffic is classified and treated as normal priority packets (best effort).</td>
</tr>
</tbody>
</table>
### WLAN-QOS-POLICY

<table>
<thead>
<tr>
<th>classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-wmm</td>
<td>Specifies how traffic from non-WMM clients is classified</td>
</tr>
<tr>
<td>voice</td>
<td>Optimized for non-WMM voice traffic. Implies all WLAN non-WMM client traffic is classified and treated as voice packets</td>
</tr>
<tr>
<td>video</td>
<td>Optimized for non-WMM video traffic. Implies all WLAN non-WMM client traffic is classified and treated as video packets</td>
</tr>
<tr>
<td>normal</td>
<td>Optimized for non-WMM best effort traffic. Implies all WLAN non-WMM client traffic is classified and treated as normal priority packets (best effort). This is the default setting.</td>
</tr>
<tr>
<td>low</td>
<td>Optimized for non-WMM background traffic. Implies all WLAN non-WMM client traffic is classified and treated as low priority packets (background)</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs7000-37FABE(config-wlan-qos-test)#classification wmm
rfs7000-37FABE(config-wlan-qos-test)#classification non-wmm video
rfs7000-37FABE(config-wlan-qos-test)#classification non-unicast normal
rfs7000-37FABE(config-wlan-qos-test)#show context wlan-qos-policy test
classification non-wmm video
classification non-unicast normal
classification non-wmm video
classification non-unicast normal
qos trust dscp
classification non-wmm wmm
accelerated-multipath autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```
### 21.1.3 multicast-mask

#### wlan-qos-policy

Configures an egress prioritization multicast mask for this WLAN QoS policy.

Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary or secondary prioritization multicast mask, the network administrator can indicate which packets are transmitted immediately.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
multicast-mask [primary|secondary] <MAC/MASK>
```

#### Parameters

- **primary <MAC/MASK>**
  - Configures the primary egress prioritization multicast mask
  - `<MAC/MASK>` – Provide the MAC address and the mask in the AA-BB-CC-DD-EE-FF /XX-XX-XX-XX-XX-XX format. The default value is 00-00-00-00-00-00/FF-FF-FF-FF-FF-FF.
  - **Note**: Setting masks is optional and only needed if there are traffic types requiring special handling.

- **secondary <MAC/MASK>**
  - Configures the secondary egress prioritization multicast mask
  - `<MAC/MASK>` – Provide the MAC address and the mask in the AA-BB-CC-DD-EE-FF /XX-XX-XX-XX-XX-XX format. The default value is 00-00-00-00-00-00/FF-FF-FF-FF-FF-FF.

#### Examples

```
rfs7000-37FABE(config-wlan-qos-test)#multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
```

```
rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
  classification non-wmm video
  multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
  classification non-unicast normal
gos trust dscp
gos trust wmm
  accelerated-multicast autodetect classification voice
  rfs7000-37FABE(config-wlan-qos-test)#
```
### 21.1.4 no

- **wlan-qos-policy**

  Negates a command or resets settings to their default

**Supported in the following platforms:**
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```markdown

no [accelerated-multicast [<IP>|autodetect]|classification {non-unicast|non-wmm}|
multicast-mask [primary|secondary]|qos trust [dscp|wmm]|svp-prioritization|
voice-prioritization]

no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold}
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|
red-threshold [background|best-effort|video|voice]}

no wmm [background|best-effort|power-save|qbss-load-element|video|voice] 
no wmm [power-save qbss-load-element] 
no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]
```

**Parameters**
- no <PARAMETERS>

  Negates a command or resets settings to their default

**Examples**

The following example shows the WLAN QoS Policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
  classification non-wmm video
  multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
  classification non-unicast normal
  qos trust dscp
  qos trust wmm
  accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

```
rfs7000-37FABE(config-wlan-qos-test)#no classification non-wmm
rfs7000-37FABE(config-wlan-qos-test)#no multicast-mask primary
rfs7000-37FABE(config-wlan-qos-test)#no qos trust dscp
```

The following example shows the WLAN QoS Policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
  classification non-unicast normal
  no qos trust dscp
  qos trust wmm
  accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```
21.1.5 qos

Enable QoS on this WLAN

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

qos trust [dscp|wmm]

Parameters

- qos trust [dscp|wmm]

|    trust [dscp|wmm] | Trusts the QoS values of ingressing packets. Both these options are enabled by default. |
|--------------------|-------------------------------------------------------------------------------------|
|                   | dscp – Trusts the IP DSCP values of ingressing packets                                |
|                   | wmm – Trusts the 802.11 WMM QoS values of ingressing packets                        |

Examples

rfs7000-37FABE(config-wlan-qos-test)#qos trust wmm
rfs7000-37FABE(config-wlan-qos-test)#qos trust dscp

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
classification non-unicast normal
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
21.1.6 rate-limit

Configure the WLAN traffic rate limits using the WLAN QoS policy.

Excessive traffic causes performance issues or brings down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server’s response. When such attributes are not present, settings defined on the controller (access point, wireless controller, or service platform) are applied. An administrator can set separate QoS rate limits for upstream (data transmitted from the managed network) and downstream (data transmitted to the managed network).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, it is recommended that you define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) are dropped resulting in intermittent outages and performance problems.

Connected wireless clients can also have QoS rate limit settings defined in both the upstream and downstream direction.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold}
rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000>}
rate-limit [client|wlan] [from-air|to-air] {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]

Parameters

- rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit client</td>
<td>Configures traffic rate limiting parameters on a per-client basis</td>
</tr>
<tr>
<td>rate-limit wlan</td>
<td>Configures traffic rate limiting parameters on a per-WLAN basis</td>
</tr>
<tr>
<td>from-air</td>
<td>Configures traffic rate limiting from a wireless client to the network</td>
</tr>
<tr>
<td>to-air</td>
<td>Configures the traffic rate limit from the network to a wireless client</td>
</tr>
<tr>
<td>max-burst-size</td>
<td>Optional. Sets the maximum burst size from 2 - 1024 kbytes. The chances of the upstream or downstream packet transmission getting congested for the WLAN’s client destination are reduced for smaller burst sizes. The default values are:</td>
</tr>
<tr>
<td>&lt;2-1024&gt;</td>
<td>- WLAN ‘to-air’ and ‘from-air’: 320 kbytes</td>
</tr>
<tr>
<td></td>
<td>- Client ‘to-air’ and ‘from-air’: 64 kbytes</td>
</tr>
<tr>
<td></td>
<td>Contd..</td>
</tr>
</tbody>
</table>
**Note:** Smaller the burst, lesser are the chances of upstream packet transmission resulting in congestion for the WLAN’s client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit [client</td>
<td>wlan] [from-air</td>
</tr>
<tr>
<td>rate &lt;50-1000000&gt;</td>
<td>Optional. Sets the traffic rate from 50 - 1000000 Kbps. This limit is the threshold value for the maximum number of packets received or transmitted over the WLAN from all access categories. Any traffic that exceeds the specified rate is dropped and a log message is generated. The default values are: - WLAN ‘to-air’ and ‘from-air’: 5000 kbytes - Client ‘to-air’ and ‘from-air’: 1000 kbytes</td>
</tr>
<tr>
<td>background &lt;0-100&gt;</td>
<td>Optional. Sets the maximum burst size from 2 - 1024 kbytes. The chances of the upstream or downstream packet transmission getting congested for the WLAN’s client destination are reduced for smaller burst sizes. The default values are: - WLAN ‘to-air’ and ‘from-air’: 320 kbytes - Client ‘to-air’ and ‘from-air’: 64 kbytes <strong>Note:</strong> Smaller the burst, lesser are the chances of upstream packet transmission resulting in congestion for the WLAN’s client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site.</td>
</tr>
<tr>
<td>best-effort &lt;0-100&gt;</td>
<td>The following is common to the ‘from-air’ and ‘to-air’ parameters: Optional. Sets a percentage value for best effort traffic in the upstream or downstream direction. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold values are: - WLAN ‘to-air’ and ‘from-air’: 50% - Client ‘to-air’ and ‘from-air’: 50%</td>
</tr>
<tr>
<td>video &lt;0-100&gt;</td>
<td>The following is common to the ‘from-air’ and ‘to-air’ parameters: Optional. Sets a percentage value for video traffic in the upstream or downstream direction. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold values are: - WLAN ‘to-air’ and ‘from-air’: 25% - Client ‘to-air’ and ‘from-air’: 25%</td>
</tr>
</tbody>
</table>
Usage Guidelines
The following information should be taken into account when configuring rate limits:

- Background traffic consumes the least bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis).
- Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).

Examples
rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air max-burst-size 6
rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air rate 55
rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air red-threshold best-effort 10
rfs7000-37FABE(config-wlan-qos-test)#rate-limit client from-air red-threshold background 3

voice <0-100>
The following is common to the ‘from-air’ and ‘to-air’ parameters:
Optional. Sets a percentage value for voice traffic in the upstream or downstream direction. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold values are:
- WLAN ‘to-air’ and ‘from-air’: 0%
- Client ‘to-air’ and ‘from-air’: 0%
Note: A value of 0% means no early random drops.
21.7 **svp-prioritization**

- **wlan-qos-policy**

Enables WLAN SVP support on this WLAN QoS policy. SVP support enables the identification and prioritization of traffic from Spectralink/Ploycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy VOIP phones. If the wireless client classification is WMM, non-WMM devices recognized as voice devices have all their traffic transmitted at voice priority. Devices are classified as voice, when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM.

This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
svp-prioritization
```

**Parameters**

None

**Examples**

```bash
rfs7000-37FABE(config-wlan-qos-test)#svp-prioritization
rfs7000-37FABE(config-wlan-qos-test)#show context wlan-qos-policy test
    classification non-wmm video
   svp-prioritization
    multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
    classification non-unicast normal
    rate-limit wlan from-air rate 55
    rate-limit wlan from-air max-burst-size 6
    rate-limit wlan from-air red-threshold best-effort 10
    rate-limit client from-air red-threshold background 3
    qos trust dscp
    qos trust wmm
    accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```
### 21.1.8 voice-prioritization

Prioritizes voice clients over other clients (for non-WMM clients). This gives priority to voice and voice management packets and is supported only on certain legacy VOIP phones. This feature is disabled by default.

Supported in the following platforms:
- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
voice-prioritization
```

**Parameters**

None

**Examples**

```plaintext
rfs7000-37FABE(config-wlan-qos-test)#voice-prioritization
rfs7000-37FABE(config-wlan-qos-test)#show context wlan-qos-policy test classification non-wmm video svp-prioritization
```

```plaintext
multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
classification non-unicast normal
rate-limit wlan from-air rate 55
rate-limit wlan from-air max-burst-size 6
rate-limit wlan from-air red-threshold best-effort 10
rate-limit client from-air red-threshold background 3
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
```

```plaintext
rfs7000-37FABE(config-wlan-qos-test)#
```
21.1.9 `wmm`

 Configures 802.11e/Wireless Multimedia (WMM) parameters for this WLAN QoS policy.

 WMM makes it possible for both home networks and Enterprises to decide which data streams are most important and assign them a higher traffic priority.

 WMM’s prioritization capabilities are based on the four access categories (background, best-effort, video, and voice). Higher the Access Category (AC) higher is the transmission probability over the controller managed WLAN. ACs correspond to the 802.1d priorities, facilitating interoperability with QoS policy management mechanisms.

 WMM enabled controllers coexist with legacy devices (not WMM-enabled).

 Packets not assigned to a specific access category are categorized as best effort by default. Applications assign each data packet to a given access category. Categorized packets are added to one of four independent transmit queues (one per access category). The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

 The same mechanism deals with external collision, to determine which client should be granted the **Opportunity to Transmit** (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category. These parameters are:

 - The minimum interframe space, or Arbitrary Inter-Frame Space Number (AIFSN)
 - The contention window, sometimes referred to as the random back off wait

 Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest back off values, they are more likely to get a TXOP.

 After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest back off value gets the TXOP.

 Supported in the following platforms:

 - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
 - Wireless Controllers — RFS4000, RFS6000, RFS7000
 - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

 **Syntax**

 `wmm [background|best-effort|power-save|qbss-load-element|video|voice]`

 `wmm [power-save|qbss-load-element]`

 `wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]`

 **Parameters**

 - `wmm [power-save|qbss-load-element]`
WLAN-QOS-POLICY 21-17

- **wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]**

| wmm | Configures 802.11e/wireless multimedia parameters. This parameter enables the configuration of four access categories. Applications assign each data packet to one of these four access categories and queues them for transmission. |
|-------------------------------------------------------------|
| background | Configures background access category parameters |
| best-effort | Configures best effort access category parameters. Packets not assigned to any particular access category are categorized by default as having best effort priority |
| video | Configures video access category parameters |
| voice | Configures voice access category parameters |
| aifsn <2-15> | Configures *Arbitrary Inter-Frame Space Number* (AIFSN) from 2 - 15. AIFSN is the wait time between data frames. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 2 The default for traffic best effort (normal) categories is 3 The default for traffic background (low) categories is 7 • <2-15> – Sets a value from 2 - 15 |
| cw-max <0-15> | Configures the maximum contention window. Wireless clients pick a number between 0 and the minimum contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 3 The default for traffic video categories is 4 The default for traffic best effort (normal) categories 10 The default for traffic background (low) categories is 10 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15. |
| cw-min <0-15> | Configures the minimum contention window. Wireless clients pick a number between 0 and the minimum contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 3 The default for traffic best effort (normal) categories is 4 The default for traffic background (low) categories is 4 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15. |
| txop-limit <0-65535> | Configures the transmit-opportunity (the interval of time during which a particular client has the right to initiate transmissions). This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 47 The default for traffic video categories is 94 The default for traffic best effort (normal) categories is 0 The default for traffic background (low) categories is 0 • <0-65535> – Set a value from 0 - 65535 to configure the transmit-opportunity in 32 microsecond units. |

**Examples**

```bash
rfs7000-37FABE(config-wlan-qos-test)#wmm video txop-limit 9
rfs7000-37FABE(config-wlan-qos-test)#wmm voice cw-min 6

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
classification non-wmm video
svp-prioritization
voice-prioritization
wmm video txop-limit 9
wmm voice cw-min 6
multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
classification non-unicast normal
rate-limit wlan from-air rate 55
rate-limit wlan from-air max-burst-size 6
rate-limit wlan from-air red-threshold best-effort 10
rate-limit client from-air red-threshold background 3
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```
CHAPTER 22
L2TPV3-POLICY

This chapter summarizes Layer 2 Tunnel Protocol Version 3 (L2TPv3) policy commands in the CLI command structure.

The L2TPv3 policy defines control and encapsulation protocols for tunneling different types of layer 2 frames between two IP nodes. The L2TPv3 control protocol controls dynamic creation, maintenance, and tear down of L2TP sessions. The L2TPV3 encapsulation protocol is used to multiplex and de-multiplex L2 data streams between two L2TP nodes across an IP network.

L2TPv3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and access point profile). L2TPv3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables WING supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between WING devices and other vendor devices supporting the L2TPv3 protocol.

Multiple pseudowires can be created within an L2TPv3 tunnel. WING supported devices support an Ethernet VLAN pseudowire type exclusively. A pseudowire is an emulation of a layer 2 point-to-point connection over a packet-switching network (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network. Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (an L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

**NOTE:** A pseudowire is an emulation of a layer 2 point-to-point connection over a packet-switching network (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (an L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TPv3 session originator and responder need to know the pseudowire type and identifier. These two parameters are communicated during L2TPv3 session establishment. An L2TPv3 session created within an L2TPv3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.
The working status of a pseudowire is reflected by the state of the L2TPv3 session. If a L2TPv3 session is down, the pseudowire associated with it must be shut down. The L2TPv3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

**NOTE:** If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

This chapter is organized into the following sections:

- `l2tpv3-policy-commands`
- `l2tpv3-tunnel-commands`
- `l2tpv3-manual-session-commands`

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
22.1 12tpv3-policy-commands

Use the (config) instance to configure L2TPv3 policy parameters. To navigate to the L2TPv3 policy instance, use the following commands:

<DEVICE>(config)#l2tpv3 policy <L2TPV3-POLICY-NAME>

rfs7000-37FABE(config)#l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

The following table summarizes L2TPv3 policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>cookie-size</td>
<td>Configures the cookie field size for each L2TPv3 data packet</td>
<td>page 22-5</td>
</tr>
<tr>
<td>failover-delay</td>
<td>Configures the L2TPv3 tunnel failover delay in seconds</td>
<td>page 22-6</td>
</tr>
<tr>
<td>force-l2-path-recovery</td>
<td>Enables the forced detection of servers and gateways behind the L2TPv3 tunnel</td>
<td>page 22-7</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Configures the interval, in seconds, between L2TPv3 &quot;Hello&quot; keep-alive messages exchanged in the L2TPv3 control connection</td>
<td>page 22-8</td>
</tr>
<tr>
<td>no</td>
<td>Negates or reverts L2TPv3 tunnel commands</td>
<td>page 22-9</td>
</tr>
</tbody>
</table>
Table 22.1 L2TPV3-Tunnel-Policy-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>reconnect-attempts</td>
<td>Configures the maximum number of retransmissions for signalling messages</td>
<td>page 22-10</td>
</tr>
<tr>
<td>reconnect-interval</td>
<td>Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection</td>
<td>page 22-11</td>
</tr>
<tr>
<td>retry-attempts</td>
<td>Configures the maximum number of retransmissions of signalling messages</td>
<td>page 22-12</td>
</tr>
<tr>
<td>retry-interval</td>
<td>Configures the interval, in seconds, before initiating a retransmission of any L2TPv3 signalling message</td>
<td>page 22-13</td>
</tr>
<tr>
<td>rx-window-size</td>
<td>Configures the number of signalling messages received without sending an acknowledgment</td>
<td>page 22-14</td>
</tr>
<tr>
<td>tx-window-size</td>
<td>Configures the number of signalling messages transmitted without receiving an acknowledgment</td>
<td>page 22-15</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
22.1.1 cookie-size

Configures the size of the cookie field present in each L2TPv3 data packet. L2TPv3 data packets contain a session cookie that identifies the session (pseudowire) corresponding to it. In a tunnel, the cookie is a 4-byte or 8-byte signature shared between the two tunnel endpoints. This signature is configured at both the source and destination routers. If the signature at both ends do not match, the data is dropped. All sessions within a tunnel have the same session cookie size.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
cookie-size [0|4|8]
```

Parameters

- `cookie-size [0|4|8]`

| `cookie-size [0|4|8]` | Configures the cookie-field size for each data packet. Select one of the following options:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No cookie field present in each L2TPv3 data message (this is the default setting)</td>
</tr>
<tr>
<td>4</td>
<td>4-byte cookie field present in each L2TPv3 data message</td>
</tr>
<tr>
<td>8</td>
<td>8-byte cookie field present in each L2TPv3 data message</td>
</tr>
</tbody>
</table>

Examples

```plaintext
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#cookie-size 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 cookie-size 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

```plaintext
no
```

Resets the cookie-field size to its default (0 - no cookie field present in each L2TPv3 data packet)
22.1.2 failover-delay

* l2tpv3-policy-commands

Configures the L2TPv3 tunnel failover delay in seconds. This is the interval after which a failed over tunnel is re-established.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
failover-delay <5-60>
```

**Parameters**

- `failover-delay <5-60>`

**Examples**

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#failover-delay 30
```

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
  hello-interval 200
  failover-delay 30
  retry-attempts 10
  retry-interval 30
  cookie-size 8
  rx-window-size 9
  tx-window-size 9
  reconnect-interval 100
  reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets the failover interval to its default (5 seconds)</td>
</tr>
</tbody>
</table>
22.1.3 force-l2-path-recovery

* **l2tpv3-policy-commands**

    Enables the forced detection of servers and gateways behind the L2TPv3 tunnel. This feature is disabled by default.

    Supported in the following platforms:

    - **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
    - **Wireless Controllers** — RFS4000, RFS6000, RFS7000
    - **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

force-l2-path-recovery

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#force-l2-path-recovery
```

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
failover-delay 30
retry-attempts 10
retry-interval 30
cookie-size 8
rx-window-size 9
tx-window-size 9
reconnect-interval 100
reconnect-attempts 8
force-l2-path-recovery
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

| **no** | Disables the forced detection of servers and gateways behind the L2TPv3 tunnel |
22.1.4 **hello-interval**

> **l2tpv3-policy-commands**

Configures the interval, in seconds, between L2TPv3 “Hello” keep-alive messages exchanged in a L2TPv3 control connection.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`hello-interval <1-3600>`

**Parameters**

- `hello-interval <1-3600>`

<table>
<thead>
<tr>
<th>hello-interval &lt;1-3600&gt;</th>
<th>Configures the interval for L2TPv3 “Hello” keep-alive messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-3600&gt; – Specify a value from 1 - 3600 seconds (default is 60 seconds).</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#hello-interval 200
```

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
  hello-interval 200
  cookie-size 8

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

- `no` resets the “Hello” keep-alive message interval to its default of 60 seconds.
22.1.5 no

- **l2tpv3-policy-commands**

Negates or reverts L2TPv3 policy settings to default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [cookie-size|failover-delay|force-l2-path-recovery|hello-interval|
   reconnect-attempts|reconnect-interval|retry-attempts|retry-interval|rx-window-size|
   tx-window-size]
```

**Parameters**

- `no <PARAMETERS>`

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Negates or reverts L2TPv3 policy settings to default</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
   hello-interval 200
   retry-attempts 10
   retry-interval 30
   cookie-size 8
   reconnect-interval 100
   reconnect-attempts 50
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no hello-interval
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-attempts
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-interval
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no retry-attempts
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no retry-interval
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no cookie-size
```

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```
22.1.6 reconnect-attempts

l2tpv3-policy-commands

Configures the maximum number of attempts made to re-establish a tunnel connection.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

reconnect-attempts <0-8>

Parameters

- reconnect-attempts <0-8>

<table>
<thead>
<tr>
<th>reconnect-attempts &lt;0-8&gt;</th>
<th>Configures the maximum number of attempts made to re-establish a tunnel connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;0-8&gt; – Specify a value from 0 - 8 (default is 0: configures infinite reconnect attempts)</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-attempts 8

rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
  hello-interval 200
  cookie-size 8
  reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

Related Commands

| no | Resets the maximum number of reconnect attempts to default (0: configures infinite reconnect attempts) |
22.1.7 **reconnect-interval**

Konfigures the interval, in seconds, between two successive attempts to re-establish a failed tunnel connection.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
reconnect-interval <1-3600>
```

**Parameters**

- reconnect-interval <1-3600>

| reconnect-interval <1-3600> | Configures the interval between successive attempts to re-establish a failed tunnel connection.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-interval 100
```

```
l2tpv3 policy L2TPV3Policy1  
  hello-interval 200  
  cookie-size 8  
  reconnect-interval 100  
  reconnect-attempts 8  
```

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

- **no**

  Resets the interval between successive attempts to re-establish a failed tunnel connection to default (120 seconds).
22.1.8 retry-attempts

*l2tpv3-policy-commands*

Configures the maximum number of attempts made to retransmit signalling messages. Use this command to specify how many retransmission cycles occur before determining the target tunnel peer is not reachable.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
retry-attempts <1-10>
```

**Parameters**

- `retry-attempts <1-10>`

**Examples**

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#retry-attempts 10
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
  hello-interval 200
  retry-attempts 10
  cookie-size 8
  reconnect-interval 100
  reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

```
no
```

Resets the maximum number of retransmissions of signalling messages to default (5 attempts)
22.1.9 retry-interval

- l2tpv3-policy-commands

Configures the interval, in seconds, between two successive attempts at retransmitting a L2TPv3 signalling message.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
retry-interval <1-250>

Parameters
- retry-interval <1-250>

<table>
<thead>
<tr>
<th>retry-interval &lt;1-250&gt;</th>
<th>Configures the interval, in seconds, between two successive retransmission attempts.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;1-250&gt; – Specify a value from 1 - 250 seconds (default is 5 seconds).</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#retry-interval 30
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context l2tpv3 policy L2TPV3Policy1
hello-interval 200
retry-attempts 10
retry-interval 30
cookie-size 8
reconnect-interval 100
reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

Related Commands
- no
  Resets the retry interval to default (5 seconds)
22.1.10 rx-window-size

`l2tpv3-policy-commands`

Configures the number of signalling packets received without sending an acknowledgment

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
rx-window-size <1-15>
```

Parameters

- `rx-window-size <1-15>`

Examples

```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#rx-window-size 9
```
```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
  hello-interval 200
  retry-attempts 10
  retry-interval 30
  cookie-size 8
  rx-window-size 9
  reconnect-interval 100
  reconnect-attempts 8
```
```
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

```
no
```

Resets the number of packets received without sending an acknowledgment to default (10 packets)
22.1.11 tx-window-size

Configures the number of signalling packets transmitted without receiving an acknowledgment

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
tx-window-size <1-15>
```

**Parameters**

- `tx-window-size <1-15>`

<table>
<thead>
<tr>
<th>tx-window-size</th>
<th>Configures the number of packets transmitted without receiving an acknowledgment</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-15&gt;</td>
<td>• &lt;1-15&gt; – Specify a value from 1 - 15 (default is 10 packets).</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#tx-window-size 9
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
  hello-interval 200
  retry-attempts 10
  retry-interval 30
  cookie-size 8
  rx-window-size 9
  tx-window-size 9
  reconnect-interval 100
  reconnect-attempts 8
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

**Related Commands**

| no | Resets the number of packets transmitted without receiving an acknowledgment to default (10 packets) |
22.2 l2tpv3-tunnel-commands

L2TPV3-POLICY

Use the (profile or device context) instance to configure a L2TPv3 tunnel. To navigate to the tunnel configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 tunnel <TUNNEL-NAME>
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 tunnel Tunnel1
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

L2tpv3 Tunnel Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>establishment-criteria</td>
<td>Set tunnel establishment criteria</td>
<td>page 22-17</td>
</tr>
<tr>
<td>fast-failover</td>
<td>Configure fast-failover support on the L2TPv3 tunnel</td>
<td>page 22-18</td>
</tr>
<tr>
<td>hostname</td>
<td>Tunnel specific local hostname</td>
<td>page 22-19</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Configure the IP address for tunnel. If not specified, tunnel source IP address would be chosen automatically based on the tunnel peer IP address</td>
<td>page 22-20</td>
</tr>
<tr>
<td>mtu</td>
<td>Configure the mtu size for the tunnel</td>
<td>page 22-21</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 22-22</td>
</tr>
<tr>
<td>peer</td>
<td>Configure the l2tpv3 tunnel peers. At least one peer must be specified</td>
<td>page 22-23</td>
</tr>
<tr>
<td>router-id</td>
<td>Tunnel specific local router ID</td>
<td>page 22-26</td>
</tr>
<tr>
<td>session</td>
<td>Create / modify the specified l2tpv3 session</td>
<td>page 22-27</td>
</tr>
<tr>
<td>use</td>
<td>Set setting to use</td>
<td>page 22-29</td>
</tr>
</tbody>
</table>

The following table summarizes L2TPv3 tunnel configuration commands:

Table 22.2 L2TPV3-Tunnel-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>establishment-criteria</td>
<td>Configures L2TPv3 tunnel establishment criteria</td>
<td>page 22-17</td>
</tr>
<tr>
<td>fast-failover</td>
<td>Configures fast-failover support on the L2TPv3 tunnel</td>
<td>page 22-18</td>
</tr>
<tr>
<td>hostname</td>
<td>Configures tunnel specific local hostname</td>
<td>page 22-19</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Configures the tunnel's IP address</td>
<td>page 22-20</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the tunnel's Maximum Transmission Unit (MTU) size</td>
<td>page 22-21</td>
</tr>
<tr>
<td>no</td>
<td>Negates or reverts L2TPv3 tunnel commands</td>
<td>page 22-22</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the tunnel's peers</td>
<td>page 22-23</td>
</tr>
<tr>
<td>router-id</td>
<td>Configures the tunnel's local router ID</td>
<td>page 22-26</td>
</tr>
<tr>
<td>session</td>
<td>Creates/modifies specified L2TPv3 session</td>
<td>page 22-27</td>
</tr>
<tr>
<td>use</td>
<td>Configures a tunnel to use a specified L2TPv3 tunnel policy</td>
<td>page 22-29</td>
</tr>
</tbody>
</table>
### 22.2.1 establishment-criteria

**l2tpv3-tunnel-commands**

Configures L2TPv3 tunnel establishment criteria

A L2TPv3 tunnel is established from the current device to the NOC controller when the current device becomes the VRRP master, cluster master, or RF Domain manager. Similarly, the L2TPv3 tunnel is closed when the current device switches to standby or backup mode.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

**Parameters**

- `establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>always</code></td>
<td>Always establishes a L2TPv3 tunnel from the current device to the NOC controller. This is the default setting. <strong>Note:</strong> The ‘always’ option indicates the device need not be a cluster-master, rf-domain-manager, or vrrp-master to establish a tunnel.</td>
</tr>
<tr>
<td><code>cluster-master</code></td>
<td>Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the cluster master <strong>Note:</strong> The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.</td>
</tr>
<tr>
<td><code>rf-domain-manager</code></td>
<td>Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the RF Domain manager <strong>Note:</strong> The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.</td>
</tr>
</tbody>
</table>
| `vrrp-master <1-255>` | Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the VRRP master  
  - `<1-255>` – Specify the VRRP group number from 1 - 255.  
  **Note:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode. |

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#establishment-criteria cluster-master
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3_tunnel Tunnell  
establishment-criteria cluster-master
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

**Related Commands**

- `no` | Resets to default (always) |
22.2.2 fast-failover

`l2tpv3-tunnel-commands`

Configures fast-failover support on the L2TPv3 tunnel. When configured, devices, using this profile, send tunnel requests to both peers, and in turn, establish tunnels with both peers. If not configured, tunnel establishment occurs on one peer, with failover and other functionality the same as legacy behavior. In case fast failover is configured when an active tunnel, with one peer, already exists, the tunnel establishment process is re-initiated with both peers. Of the two tunnels established, one is marked active while the other is standby. The sessions and routes from the active tunnel are only pushed to the dataplane, resulting in creation of data sessions. However, if the active tunnel fails, sessions and routes from the standby tunnel are pushed to the dataplane thereby providing almost immediate fail over. Both tunnels individually perform connection health checkups through hello intervals. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

`fast-failover {aggressive}`

Parameters

- `fast-failover {aggressive}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggressive</td>
<td>Optional. When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of the number of retry attempts configured. This option is disabled by default. <strong>Note:</strong> The <code>hello-interval</code> and <code>retry-attempts</code> parameters are defined in the L2TPv3 Policy context. For more information on configuring an L2TPv3 policy, see <code>l2tpv3-policy-commands</code>. For more information on associating an L2TPv3 policy to an L2TPv3 tunnel, see <code>use</code>.</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809(config-profile testNX9000-l2tpv3-tunnel-TestTunnel2)#show context include-factory | include fast-failover
   no fast-failover
nx9500-6C8809(config-profile testNX9000-l2tpv3-tunnel-TestTunnel2)#

nx9500-6C8809(config-profile testNX9000-l2tpv3-tunnel-TestTunnel2)#fast-failover aggressive

nx9500-6C8809(config-profile testNX9000-l2tpv3-tunnel-TestTunnel2)#show context l2tpv3_tunnel TestTunnel2 fast-failover aggressive
nx9500-6C8809(config-profile testNX9000-l2tpv3-tunnel-TestTunnel2)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes fast-failover support on the L2TPv3 tunnel</td>
</tr>
</tbody>
</table>
### 22.2.3 hostname

- **l2tpv3-tunnel-commands**

 Configures the tunnel’s local hostname

 Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
hostname <WORD>
```

**Parameters**

- hostname <WORD>

<table>
<thead>
<tr>
<th>hostname &lt;WORD&gt;</th>
<th>Configures the tunnel’s local hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>Specify the tunnel’s local hostname.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#hostname TunnelHost1
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
   hostname TunnelHost1
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

**Related Commands**

```
no
```

<table>
<thead>
<tr>
<th>no</th>
<th>Removes the tunnel’s local hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 22.2.4 `local-ip-address`

`l2tpv3-tunnel-commands`

Configures the tunnel's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel's peer IP address.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`local-ip-address <IP>`

**Parameters**

- `local-ip-address <IP>`

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#local-ip-address 172.16.10.2
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

**Related Commands**

- `no`
  Resets the tunnel's local IP address and re-establishes the tunnel
22.2.5 mtu

Configures the MTU size for this tunnel. This value determines the packet size transmitted over this tunnel.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
mtu <128-1460>

Parameters
- mtu <128-1460>

<table>
<thead>
<tr>
<th>mtu &lt;128-1460&gt;</th>
<th>Configures the MTU size for this tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;128-1460&gt; – Specify a value from 128 - 1460 bytes (default is 1460 bytes).</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#mtu 1280

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  mtu 1280
  hostname TunnelHost1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#

Related Commands

| no | Resets the MTU size for this tunnel to default (1460 bytes) |
22.2.6 no

Negates or reverts a L2TPv3 tunnel settings to default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [establishment-criteria|fast-failover|hostname|local-ip-address|mtu|peer <1-2>|router-id|session|use]

Parameters

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Negates or reverts a L2TPv3 tunnel settings to default</th>
</tr>
</thead>
</table>

Examples

The tunnel settings before the 'no' command is executed:

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
local-ip-address 172.16.10.2
mtu 1280
hostname TunnelHost1
establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#

The tunnel settings after the 'no' command is executed:

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no local-ip-address
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no mtu
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no hostname

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
22.2.7 peer

- **l2tpv3-tunnel-commands**

Configures the L2TPv3 tunnel’s peers. At least one peer must be specified.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```
peer <1-2> {hostname|ip-address|ipsec-secure|router-id|udp}
peer <1-2> {hostname [any]} {ipsec-secure|router-id|udp}
peer <1-2> {ip-address <IP>} {hostname|ipsec-secure|router-id|udp}
peer <1-2> {ipsec-secure} {gw [IP|<WORD>]}
peer <1-2> {router-id [IP|<WORD>]} {ipsec-secure|udp}
peer <1-2> {udp} {ipsec-secure|port <1-65535>}
```

### Parameters

- **peer <1-2>**

Configures the tunnel’s peer ID from 1 - 2. The peer ID identifies the primary (ID 1) secondary (ID 2) peers. The L2TPv3 tunnel is established with the primary peer. The secondary peer is used for tunnel failover. If the peer is not specified, tunnel establishment does not occur.

**Note:** At any time the tunnel is established with only one peer, unless fast-failover support is configured on the L2TPv3 tunnel. For more information, see fast-failover.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname [any]</td>
<td>Optional. Configures the peers’ hostname. The hostname options are:</td>
</tr>
<tr>
<td></td>
<td>- &lt;HOSTNAME&gt; – Specifies the hostname as <strong>Fully Qualified Domain Name</strong> (FQDN) or partial DN or any other name</td>
</tr>
<tr>
<td></td>
<td>- any – Peer name is not specified. If the hostname is ‘any’ this tunnel is considered as responder only and will allow incoming connection from any host.</td>
</tr>
<tr>
<td>ipsec-secure {gw [IP</td>
<td>&lt;WORD&gt;]}</td>
</tr>
<tr>
<td></td>
<td>- ipsec-secure – Enables auto IPSec on the L2TPv3 tunnel</td>
</tr>
<tr>
<td></td>
<td>- gw – Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:</td>
</tr>
<tr>
<td></td>
<td>- &lt;IP&gt; – Configures IPSec gateway’s IP address</td>
</tr>
<tr>
<td>router-id [any]</td>
<td>After specifying the peer hostname, optionally specify router ID settings:</td>
</tr>
<tr>
<td></td>
<td>- router-id – Configures the peer’s router ID in one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>- &lt;IP&gt; – Peer router ID in the IP address (A.B.C.D) format</td>
</tr>
<tr>
<td></td>
<td>- &lt;WORD&gt; – Peer router ID range (for example, 100-120)</td>
</tr>
<tr>
<td></td>
<td>- any – Peer router ID is not specified. This allows incoming connection from any router ID.</td>
</tr>
</tbody>
</table>
peer <1-2> \{ip-address <IP>\} \{hostname|ipsec-secure|router-id|udp\}

peer <1-2> Configures the tunnel’s peer ID from 1 - 2. At any time the tunnel is established with only one peer.

ip-address <IP> Optional. Configures the peer’s IP address in the A.B.C.D format
- <IP> – Specify the peer’s IP address.

hostname \[<FQDN>|any\] After specifying the peer IP address, optionally specify the peer’s hostname:
- hostname – Optional. Configures the peers’ hostname. The hostname options are:
  - <FQDN> – Specifies the host name as FQDN or partial DN
  - any – Peer name is not specified. If the hostname is ‘any’ this tunnel is considered as responder only and will allow incoming connection from any host.

ipsec-secure \{gw \[<IP>|<WORD>\]\} After specifying the peer IP address, optionally specify the IPSec settings:
- ipsec-secure – Optional. Enables auto IPSec
  - gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:
    - <IP> – Configures IPSec gateway’s IP address
    - <WORD> – Configures IPSec gateway’s hostname

router-id \[<A.B.C.D>|<WORD>|any\] After specifying the peer IP address, optionally specify the router ID using one of the following options:
- router-id – Optional. Configures the peer’s router-id in one of the following formats:
  - <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format
  - <WORD> – Peer router ID range (for example, 100-120)
  - any – Peer router ID is not specified. This allows incoming connection from any router ID.

udp \{ipsec-secure gw\} \{port <1-65535> \{ipsec-secure\}\} After specifying the peer IP address, optionally specify the peer’s UDP port settings:
The UDP option configures the encapsulation mode for this tunnel.
- UDP – Optional. Configures UDP encapsulation (default encapsulation is IP)
  - ipsec-secure gw – Optional. Enables auto IPSec
  - port <1-65535> – Optional. Configures the peer’s UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

peer <1-2> \{ipsec-secure\} \{gw \[<IP>|<WORD>\]\} Optional. Enables auto IPSec for this peer
- gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:
  - <IP> – Configures IPSec gateway’s IP address
  - <WORD> – Configures IPSec gateway’s hostname
peer <1-2> [router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}

peer <1-2>
Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.

router-id [A.B.C.D]|<WORD>|any] Optional. Configures the peer’s router-id in one of the following formats:
• A.B.C.D – Peer router ID in the IP address (A.B.C.D) format
• <WORD> – Peer router ID range (for example, 100-120)
• any – Peer router ID is not specified. This allows incoming connection from any router ID.

ipsec-secure gw [<IP>|<WORD>]} After specifying the peer’s router ID, optionally specify the IPSec settings.
• ipsec-secure – Optional. Enables auto IPSec
  • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:
    • <IP> – Configures IPSec gateway’s IP address
    • <WORD> – Configures IPSec gateway’s hostname

udp [ipsec-secure gw] port <1-65535> {ipsec-secure} After specifying the peer’s router ID, optionally specify the IPSec settings.
The UDP option configures the encapsulation mode for this tunnel.
• UDP – Optional. Configures UDP encapsulation (default encapsulation is IP)
  • ipsec-secure gw – Optional. Enables auto IPSec
  • port <1-65535> – Optional. Configures the peer’s UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

Examples
rfs7000-37FABE (config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1) # peer 2
hostname tunnel1peer1 udp port 100

rfs7000-37FABE (config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1) # show context
l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  establishment-criteria cluster-master
rfs7000-37FABE (config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1) #

Related Commands
no Removes the peer configured for this tunnel
22.2.8 **router-id**

Configures the tunnel’s local router ID

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`router-id [1-4294967295]|<IP>`

**Parameters**

- `router-id [1-4294967295]|<IP>`

| **router-id [1-4294967295]|<IP>** | Configures the tunnel’s local router ID in one of the following formats: |
|-------------------------------------|---------------------------------------------------------------|
|                                    | • `1-4294967295` – Router ID in the number format (from 1 - 4294967295) |
|                                    | • `<IP>` – Router ID in IP address format (A.B.C.D) |

**Examples**

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#router-id 2000

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  router-id 2000
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#

**Related Commands**

- `no` Removes the tunnel’s router ID
22.2.9 session

- **l2tpv3-tunnel-commands**

Configures a session’s pseudowire ID, which describes the session’s purpose. The session established message sends this pseudowire ID to the L2TPv3 peer.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
session <L2TPV3-SESSION-NAME> [pseudowire-id|rate-limit]
```

```
session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
  vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

```
session <L2TPV3-SESSION-NAME> rate-limit [egress|ingress] rate <50-1000000>
  max-burst-size <2-1024>
```

**Parameters**

- `session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}`

<table>
<thead>
<tr>
<th>session &lt;L2TPV3-SESSION-NAME&gt;</th>
<th>Configures this session’s name</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;L2TPV3-SESSION-NAME&gt; – Specify the L2TPV3 session name (should not exceed 31 characters in length). A tunnel is usable only if it has one or more session(s) (having specific session names) configured. The L2TPv3 tunnel has no idle timeout, it closes when the last tunnel session is closed.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pseudowire-id &lt;1-4294967295&gt;</th>
<th>Configures the pseudowire ID for this session from 1- 4204067295</th>
</tr>
</thead>
<tbody>
<tr>
<td>A pseudowire is an emulation of a layer 2 point-to-point connection over a packet-switching network (PSN). A pseudowire is needed to encapsulate and tunnel layer 2 protocols across a layer 3 network.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>traffic-source vlan &lt;VLAN-ID-RANGE&gt;</th>
<th>Configures VLAN as the traffic source for this tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;VLAN-ID-RANGE&gt; – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>native-vlan &lt;1-4094&gt;</th>
<th>Optional – Configures the native VLAN ID for this session, which is not tagged</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;1-4094&gt; – Specify the native VLAN ID from 1- 4094.</td>
<td></td>
</tr>
</tbody>
</table>

- `session <L2TPV3-SESSION-NAME> rate-limit [egress|ingress] rate <50-1000000> max-burst-size <2-1024>`
Usage Guidelines
The working status of a pseudowire is reflected by the state of the L2TPv3 session. If the corresponding session is L2TPv3 down, the pseudowire associated with it must be shut down.

Examples
```
   rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#session
tunnellpeer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
```
```
   rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
   l2tpv3 tunnel Tunnel1
   peer 2 hostname tunnellpeerin1 udp port 100
   session tunnellpeerin1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
   router-id 2000
   establishment-criteria cluster-master
```

Related Commands
```
no
```
Removes a session
### 22.2.10 use

* **l2tpv3-tunnel-commands**

Configures a tunnel to use a specified L2TPv3 tunnel policy and specified critical resources

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
use [critical-resource|l2tpv3-policy]
use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}
use l2tpv3-policy <L2TPV3-POLICY-NAME>
```

#### Parameters

- **use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}**
  - Specifies the critical resource(s) to use with this tunnel
  - `<CRM1-NAME>` – Specify the first critical resource name (should be existing).
  - `<CRM-NAME2/3/4>` – Optional. Specify the second/third/fourth critical resource names. Maximum of four critical resources can be monitored.

  **Note:** In case of tunnel initiator, L2TPv3 tunnel is established only if the critical resources identified by the `<CRM-NAME1>.............. <CRM-NAME4>` arguments are available at the time of tunnel establishment.

  **Note:** In case of L2TPv3 tunnel termination, all incoming tunnel establishment requests are rejected if the critical resources specified by the `<CRM-NAME1>.............. <CRM-NAME4>` arguments are not available.

- **use l2tpv3-policy <L2TPV3-POLICY-NAME>**
  - Associates a specified L2TPv3 policy with this tunnel
  - `<L2TPV3-POLICY-NAME>` – Specify the policy name (should be existing and configured).

#### Examples

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#use l2tpv3-policy L2TPV3Policy1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnellpeer1 udp port 100
  use l2tpv3-policy L2TPV3Policy1
  session tunnellpeer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
  router-id 2000
  establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

#### Related Commands

- **no**
  - Removes the L2TPv3 policy configured with a tunnel and reverts to the default tunnel policy
22.3 l2tpv3-manual-session-commands

L2TPV3-POLICY

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

Use the (profile-context) instance to manually configure a L2TPv3 session. To navigate to the L2TPv3 manual session configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 manual-session <SESSION-NAME>
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 manual-session test
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#?
```

L2tpv3 Manual Session Mode commands:

- `local-cookie`: The local cookie for the session.
- `local-ip-address`: Configure the IP address for tunnel. If not specified, tunnel source ip address would be chosen automatically based on the tunnel peer ip address.
- `local-session-id`: Local session id for the session.
- `mtu`: Configure the mtu size for the tunnel.
- `no`: Negate a command or set its defaults.
- `peer`: Configure L2TPv3 manual session peer.
- `remote-cookie`: The remote cookie for the session.
- `remote-session-id`: Remote session id for the session.
- `traffic-source`: Traffic that is tunneled.
- `clrscr`: Clears the display screen.
- `commit`: Commit all changes made in this session.
- `end`: End current mode and change to EXEC mode.
- `exit`: End current mode and down to previous mode.
- `help`: Description of the interactive help system.
- `revert`: Revert changes.
- `service`: Service Commands.
- `show`: Show running system information.
- `write`: Write running configuration to memory or terminal.

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

The following table summarizes L2TPv3 manual session configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local-cookie</code></td>
<td>Configures the manual session’s local cookie field size</td>
<td>page 22-31</td>
</tr>
<tr>
<td><code>local-ip-address</code></td>
<td>Configures the manual session’s local source IP address</td>
<td>page 22-32</td>
</tr>
<tr>
<td><code>local-session-id</code></td>
<td>Configures the manual session’s local session ID</td>
<td>page 22-33</td>
</tr>
<tr>
<td><code>mtu</code></td>
<td>Configures the MTU size for the manual session tunnel</td>
<td>page 22-34</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negates or reverts L2TPv3 manual session commands to default</td>
<td>page 22-22</td>
</tr>
<tr>
<td><code>peer</code></td>
<td>Configures the manual session’s peers</td>
<td>page 22-36</td>
</tr>
<tr>
<td><code>remote-cookie</code></td>
<td>Configures the remote cookie for the manual session</td>
<td>page 22-37</td>
</tr>
<tr>
<td><code>remote-session-id</code></td>
<td>Configures the manual session’s remote session ID</td>
<td>page 22-38</td>
</tr>
<tr>
<td><code>traffic-source</code></td>
<td>Configures the traffic source tunneled by the manual session</td>
<td>page 22-39</td>
</tr>
</tbody>
</table>
22.3.1 local-cookie

 Configures the local cookie field size for the manual session

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

local-cookie size [4|8] <1-4294967295> {<1-4294967295>}

Parameters

- local-cookie size [4|8] <1-4294967295> {<1-4294967295>}

| local-cookie size [4|8] | Configures the local cookie field size for this manual session. The options are: |
|-------------------------|-----------------------------------------------------------------------------------|
|                        | • 4 – 4 byte local cookie field                                                   |
|                        | • 8 – 8 byte local cookie field                                                   |

| <1-4294967295>         | Configures the local cookie value first word. Applies to both the 4 byte and 8 byte local cookies |

| <1-4294967295>         | Optional – Configures the local cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies. |

Examples

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#local-cookie size 8 200 300

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test

local-cookie size 8 200 300

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

Related Commands

| no                      | Removes the local cookie size configured for a manual session |
22.3.2 local-ip-address

Configures the manual session’s source IP address. If no IP address is specified, the tunnel’s source IP address is automatically configured based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

local-ip-address <IP>

Parameters

- **local-ip-address <IP>**

<table>
<thead>
<tr>
<th>local-ip-address &lt;IP&gt;</th>
<th>Configures the manual session’s source IP address in the A.B.C.D format</th>
</tr>
</thead>
</table>

Examples

```
   rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#local-ip-address 1.2.3.4
   rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
   local-cookie size 8 200 300
   local-ip-address 1.2.3.4
   rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

- **no** | Resets the manual session’s local source IP address. This re-establishes the session. |
### 22.3.3 `local-session-id`

- **`l2tpv3-manual-session-commands`**

  Configures the manual session’s local session ID

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

`local-session-id <1-63>`

**Parameters**

- `local-session-id <1-63>`

| `local-session-id <1-63>` | Configures this manual session’s local session ID from 1 - 63. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer. |

**Examples**

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

**Related Commands**

- `no` Removes the manual session's local session ID
22.3.4 mtu

`l2tpv3-manual-session-commands`

Configures the MTU size for the manual session tunnel. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mtu <128-1460>
```

**Parameters**

- `mtu <128-1460>`

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#mtu 200
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  mtu 200
  local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

**Related Commands**

```
no
```

Resets the MTU size for this manual session to default (1460 bytes)
22.3.5 no

Negates or reverts L2TPv3 manual session settings to default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|remote-session-id|traffic-source]

Parameters

- no <PARAMETERS>

Examples

The following example shows the manual session 'test' settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no local-ip-address
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no local-session-id
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no remote-session-id
```

The following example shows the manual session 'test' settings after the 'no' commands are executed:

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```
### 22.3.6 peer

#### l2tpv3-manual-session-commands

Configures peer(s) allowed to establish the manual session tunnel. The peers are identified by their IP addresses.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
peer ip-address <IP> {udp {port <1-65535>}}
```

#### Parameters

- **peer ip-address <IP> {udp {port <1-65535>}}**

<table>
<thead>
<tr>
<th>peer ip-address &lt;IP&gt;</th>
<th>Configures the tunnel’s peer IP address in the A.B.C.D format</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp {port &lt;1-65535&gt;}</td>
<td>Optional. Configures the UDP encapsulation mode for this tunnel (default encapsulation is IP)</td>
</tr>
<tr>
<td></td>
<td>• port &lt;1-65535&gt; – Optional. Configures the peer’s UDP port running the L2TPv3 service.</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Specify a value from 1 - 65535.</td>
</tr>
</tbody>
</table>

#### Examples

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#peer ip-address 5.6.7.8 udp port 150
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
local-cookie size 8 200 300
local-ip-address 1.2.3.4
peer ip-address 5.6.7.8 udp port 150
mtu 200
local-session-id 1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

#### Related Commands

- **no** Removes the manual session’s peer
22.3.7 **remote-cookie**

> l2tpv3-manual-session-commands

Configures the manual session’s remote cookie field size

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}

**Parameters**

- remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}

| remote-cookie size [4|8] | Configures the remote cookie field size for this manual session. The options are: |
|--------------------------|---------------------------------------------------------------------------------|
|                          | • 4 – 4 byte remote cookie field                                                  |
|                          | • 8 – 8 byte remote cookie field                                                  |
| <1-4294967295>           | Configures the remote cookie value first word. Applies to both the 4 byte and 8 byte local cookies |
| <1-4294967295>           | Optional – Configures the remote cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies. |

**Examples**

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#remote-cookie size 8 400 700

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  mtu 200
  local-session-id 1
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>no</th>
<th>Removes the manual session’s remote cookie field size</th>
</tr>
</thead>
</table>
22.3.8 remote-session-id

Configures the manual session’s remote ID. This ID is passed in the establishment of the tunnel session.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
remote-session-id <1-4294967295>

Parameters
- remote-session-id <1-4294967295>

Examples
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#remote-session-id 200

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

Related Commands
- no
  Removes the manual session’s remote ID
### 22.3.9 traffic-source

* `l2tpv3-manual-session-commands`

Configures the traffic source tunneled by this session

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

**Parameters**

- `traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-source vlan</td>
<td>Configures VLAN as the traffic source for this tunnel</td>
</tr>
<tr>
<td>&lt;VLAN-ID-RANGE&gt;</td>
<td>• &lt;VLAN-ID-RANGE&gt; — Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35)</td>
</tr>
<tr>
<td>native-vlan &lt;1-4094&gt;</td>
<td>Optional – Configures the native VLAN ID for this session, which is not tagged</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the native VLAN ID from 1-4094.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#traffic-source vlan 50-60 native-vlan 2
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

**Related Commands**

- `no`
  - Removes the traffic source configured for a tunnel
CHAPTER 23
ROUTER-MODE COMMANDS

This chapter summarizes Open Shortest Path First (OSPF) router mode commands in the CLI command structure. All router-mode commands are available on both device and profile modes.

OSPF is an interior gateway protocol (IGP) used within large autonomous systems to distribute routing information. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers. This enables routers to synchronize routing tables.

OSPF uses a route table managed by the link cost (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability.

Use the (config) instance to configure router commands. To navigate to the (config-router-mode) instance, use the following command:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#router ospf
<DEVICE>(config-profile <PROFILE-NAME>-router-ospf)#
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#router ospf
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#?

Router OSPF Mode commands:
- `area` OSPF area
- `auto-cost` OSPF auto-cost
- `default-information` Distribution of default information
- `ip` Internet Protocol (IP)
- `network` OSPF network
- `no` Negate a command or set its defaults
- `ospf` OSPF
- `passive` Make OSPF Interface as passive
- `redistribute` Route types redistributed by OSPF
- `route-limit` Limit for number of routes handled OSPF process
- `router-id` Router ID
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
</tr>
</tbody>
</table>

**rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#**

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
23.1 router-mode

The following table summarizes router configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Specifies OSPF enabled interfaces</td>
<td>page 23-4</td>
</tr>
<tr>
<td>auto-cost</td>
<td>Specifies the reference bandwidth in terms of Mbits per second</td>
<td>page 23-14</td>
</tr>
<tr>
<td>default-information</td>
<td>Controls the distribution of default information</td>
<td>page 23-15</td>
</tr>
<tr>
<td>ip</td>
<td>Configures Internet Protocol (IP) default gateway priority</td>
<td>page 23-16</td>
</tr>
<tr>
<td>network</td>
<td>Defines OSPF network settings</td>
<td>page 23-17</td>
</tr>
<tr>
<td>ospf</td>
<td>Enables OSPF</td>
<td>page 23-18</td>
</tr>
<tr>
<td>passive</td>
<td>Specifies the configured OSPF interface as passive interface</td>
<td>page 23-19</td>
</tr>
<tr>
<td>redistribute</td>
<td>Specifies the route types redistributed by OSPF</td>
<td>page 23-20</td>
</tr>
<tr>
<td>route-limit</td>
<td>Specifies the limit for the number of routes managed by OSPF</td>
<td>page 23-21</td>
</tr>
<tr>
<td>router-id</td>
<td>Specifies the router ID for OSPF</td>
<td>page 23-22</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its defaults</td>
<td>page 23-23</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
23.1.1 area

router-mode

Configures OSPF network area (OSPF enabled interfaces) settings

The following table lists the OSPF Area configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Creates a new OSPF area and enters its configuration mode</td>
<td>page 23-5</td>
</tr>
<tr>
<td>OSPF-area-mode</td>
<td>Summarizes OSPF area configuration commands</td>
<td>page 23-8</td>
</tr>
</tbody>
</table>
23.1.1.1 area

area

Configures OSPF network areas (OSPF enables interfaces)

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can be defined as: stub area, totally-stub, non-stub, nssa, totally nssa. Each of these area types has been discussed further in the area-type section of this chapter.

At least one default area, bearing number '0', should be configured for every OSPF network. In case of multiple areas, the default area 0 forms the backbone of the network. The default area 0 is used as a link to the other areas. Each area has its own link-state database.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

Supported in the following platforms:
• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
• Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax
area [<0-4294967295>|<IP>]

Parameters
• area [<0-4294967295>|<IP>]

<table>
<thead>
<tr>
<th>area</th>
<th>Defines an OSPF area</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>Defines an OSPF area in the form of a 32 bit integer</td>
</tr>
<tr>
<td>• &lt;0-4294967295&gt; – Specify the value from 0 - 4294967295.</td>
<td></td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Defines an OSPF area in the form of an IP address</td>
</tr>
<tr>
<td>• &lt;IP&gt; – Specify the IP address.</td>
<td></td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#area 4 ?
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#?

Router OSPF Area Mode commands:
• area-type OSPF area type
• authentication Authentication scheme for OSPF area
• no Negate a command or set its defaults
• range Routes matching this range are considered for summarization (ABR only)
• clrscr Clears the display screen
• commit Commit all changes made in this session
• do Run commands from Exec mode
• end End current mode and change to EXEC mode
• exit End current mode and down to previous mode
• help Description of the interactive help system
• revert Revert changes
• service Service Commands
• show Show running system information
• write Write running configuration to memory or terminal
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#show context
area 0.0.0.4
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes area configuration settings</td>
</tr>
</tbody>
</table>
23.1.1.2 OSPF-area-mode

The following table summarizes OSPF area mode configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-type</td>
<td>Configures a particular OSPF area as STUB or NSSA</td>
<td>page 23-9</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the authentication scheme used for the OSPF area</td>
<td>page 23-11</td>
</tr>
<tr>
<td>range</td>
<td>Specifies the routes matching address/mask for summarization</td>
<td>page 23-12</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its defaults</td>
<td>page 23-13</td>
</tr>
</tbody>
</table>
23.1.1.2.1 area-type

OSPF-area-mode

Configures a particular OSPF area type as STUB, Totally STUB, NSSA or Totally NSSA.

Areas can be defined as:

- **stub area** - Is an area that does not receive route advertisements external to the autonomous system (AS), and routing from within the area is based entirely on a default route.
- **totally-stub** - Is an area that does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there is only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- **non-stub** - Is an area that imports autonomous system external routes and forwards to other areas. However, it still cannot receive external routes from other areas.
- **nssa** - A Not-So-Stubby Area (NSSA) is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.
- **totally-nssa** - Is a NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an Autonomous System Boundary Router (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

Supported in the following platforms:

- **Access Points** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000

**Syntax**

- `area-type nssa|stub`
- `area-type nssa {default-cost|no-summary|translate-always|translate-candidate|translate-never}`
- `area-type nssa {default-cost <0-16777215> {no-summary}|no-summary {default-cost <0-16777215>}}`
- `area-type nssa {translate-always|translate-candidate|translate-never} {(default-cost <0-16777215>|no-summary)}`
- `area-type stub {default-cost <0-16777215> {no-summary}|no-summary {default-cost <0-16777215>}}`

**Parameters**

- **area-type [nssa|stub] {default-cost|no-summary|translate-always|translate-candidate|translate-never}**

<table>
<thead>
<tr>
<th>area-type</th>
<th>Configures a particular OSPF area type as STUB, Totally STUB, NSSA or Totally NSSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>nssa</td>
<td>Configures the OSPF area as NSSA</td>
</tr>
<tr>
<td>stub</td>
<td>Configures the OSPF area as Stubby Area (STUB)</td>
</tr>
<tr>
<td>default-cost</td>
<td>Specifies the default summary cost that will be advertised, if the OSPF area is a STUB or NSSA</td>
</tr>
<tr>
<td>&lt;0-16777215&gt;</td>
<td>&lt;0-16777215&gt; -- Specify the default summary cost value from 0 - 16777215.</td>
</tr>
<tr>
<td>no-summary</td>
<td>Configures the OSPF area as totally STUB if the area-type is STUB or totally NSSA if the area-type is NSSA</td>
</tr>
<tr>
<td>translate-always</td>
<td>Always translates type-7 Link State Advertisements (LSAs) into type-5 LSAs</td>
</tr>
</tbody>
</table>
### translate-candidate
- Defines it as default behavior

### translate-never
- Never translates type-7 LSAs into type-5 LSAs

#### Examples
```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#area-type stub
default-cost 1
```
```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show context area 0.0.0.1
  area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

#### Related Commands
```
no
- Removes configured area-type settings
```
23.1.2.2 authentication

OSPF-area-mode

Specifies an authentication scheme used for an OSPF area used with the OSPF dynamic route.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

authentication [message-digest|simple-password]

Parameters

- authentication [message-digest|simple-password]

<table>
<thead>
<tr>
<th>message-digest</th>
<th>Configures the message-digest (MD-5) authentication scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple-password</td>
<td>Configures the simple password authentication scheme</td>
</tr>
</tbody>
</table>

Usage Guidelines

OSPF packet authentication enables routers to use predefined passwords and participate within a routing domain. The two authentication modes are:
- MD-5 — MD-5 authentication is a cryptographic authentication mode, where every router has a key (password) and key-id configured on it. This key and key-id together form the message digest that is appended to the OSPF packet.
- Simple Password — Simple password authentication allows a password (key) to be configured per area. Routers in the same area and participating in the routing domain have to be configured with the same key.

Examples

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#authentication simple-password

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show context area 0.0.0.1
  authentication simple-password
  area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#

Related Commands

| no | Removes the authentication scheme |
23.1.1.2.3 range

OSPF-area-mode

Specifies a range of addresses for routes matching address/mask for OSPF summarization

Supported in the following platforms:
  • Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  • Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax
range <IP/M>

Parameters
• range <IP/M>

<table>
<thead>
<tr>
<th>&lt;IP/M&gt;</th>
<th>Specifies the routes matching address/mask for summarization. Note: This command is applicable for an Area Border Router (ABR) only.</th>
</tr>
</thead>
</table>

Examples
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#range 172.16.10.0/24
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show context area 0.0.0.1
  authentication simple-password
  range 172.16.10.0/24
  area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#

Related Commands
no

Removes the configured network IP range
23.1.2.4 no

- **OSPF-area-mode**

  Negates a command or set its defaults

  Supported in the following platforms:
  - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

```plaintext
no [area-type|authentication|range]
```

**Parameters**

- `no <PARAMETERS>`

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Negates a command or set its defaults</th>
</tr>
</thead>
</table>

**Usage Guidelines**

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

**Examples**

The following example shows the OSPF router settings before the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show context
area 0.0.0.1
  authentication simple-password
  range 172.16.10.0/24
  area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#

rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#no authentication
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#no range 172.16.10.0/24
```

The following example shows the OSPF router settings after the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show context
area 0.0.0.1
  area-type stub default-cost 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```
23.1.2 auto-cost

`router-mode`

Configures the reference bandwidth in terms of megabits per second. Specifying the reference bandwidth allows you to control the default metrics for an interface, which is calculated by OSPF.

The formula used to calculate default metrics is: \( \text{ref-bw} \) divided by the \( \text{bandwidth} \).

Use the `no > auto-cost > reference-bandwidth` command to configure default metrics calculation based on interface type.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

`auto-cost reference-bandwidth <1-4294967>`

**Parameters**

- `reference-bandwidth <1-4294967>`

**Examples**

```bash
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#auto-cost reference-bandwidth 1
```

Please make sure that auto-cost reference-bandwidth is configured uniformly on all routers.

```bash
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

```bash
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context router ospf
        area 0.0.0.4
        auto-cost reference-bandwidth 1
        rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

**Related Commands**

- `no` Removes auto-cost reference bandwidth settings
23.1.3 default-information

- router-mode

Controls the distribution of default route information. Use the default-information > originate command to advertise a default route in the routing table.

This option is disabled by default. When enabled, the default route becomes a distributed route.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

default-information originate {always|metric|metric-type}
default-information originate {always|metric <0-16777214>|metric-type [1|2]}
{((metric <0-16777214>|metric-type [1|2]))}

Parameters
- default-information originate {always|metric <0-16777214>|metric-type [1|2]}
{((metric <0-16777214>|metric-type [1|2]))}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>originate</td>
<td>Originates default route information. Enabling this feature makes the default route a distributed route. This option is disabled by default.</td>
</tr>
<tr>
<td>always</td>
<td>Optional. Always distributes default route information (will continue to advertise default route information even if that information has been removed from the routing table for some reason). This option is disabled by default.</td>
</tr>
<tr>
<td>metric &lt;0-16777214&gt;</td>
<td>This is a recursive parameter and can be optionally configured along with the metric-type option.</td>
</tr>
<tr>
<td></td>
<td>• metric &lt;0-16777214&gt; – Optional. Specifies OSPF metric value for redistributed routes (this value is used to generate the default route)</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-16777214&gt; – Specify a value from 0 - 16777214.</td>
</tr>
<tr>
<td>metric-type [1</td>
<td>2]</td>
</tr>
<tr>
<td></td>
<td>• metric-type [1</td>
</tr>
<tr>
<td></td>
<td>• 1 – Sets OSPF external type 1 metrics</td>
</tr>
<tr>
<td></td>
<td>• 2 – Sets OSPF external type 2 metrics</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#default-information originate metric-type 2 metric 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context router ospf
area 0.0.0.4
auto-cost reference-bandwidth 1
default-information originate metric 1 metric-type 2
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#

Related Commands

no Disables advertising of default route information available in the routing table
### 23.1.4 ip

**router-mode**

Configures IP default gateway priority

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

```
ip default-gateway priority <1-8000>
```

**Parameters**

- ip default-gateway priority <1-8000>

<table>
<thead>
<tr>
<th>default-gateway priority &lt;1-8000&gt;</th>
<th>Configures the default gateway priority &lt;1-8000&gt; for the default gateway acquired via OSPF. This parameter sets the priority, with a lower value indicating a higher priority. The default value is 7000.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#ip default-gateway priority 1
```

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context router ospf
area 0.0.0.4
auto-cost reference-bandwidth 1
default-information originate metric 1 metric-type 2
ip default-gateway priority 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>no</th>
<th>Removes default gateway priority settings</th>
</tr>
</thead>
</table>
23.1.5 network

Assigns networks to specified areas (defines the OSPF interfaces and their associated area IDs)

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

```
network <IP/M> area [0-4294967295]<IP>
```

Parameters

- **network <IP/M> area [0-4294967295]<IP>**

| <IP/M> | Specifies an OSPF network address/mask value. Defines networks (IP addresses and mask) participating in OSPF. |
| area [0-4294967295]<IP> | Specifies an OSPF area, associated with the OSPF address range, in one of the following formats:  
  - <0-4294967295> – Specifies a 32 bit OSPF area ID from 0 - 4294967295  
  - <IP> – Defines an OSPF area ID in the form of an IPv4 address |

Examples

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#network 1.2.3.0/24 area 4.5.6.7
```

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context router ospf
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
  rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

| **no** | Removes the OSPF network to area ID association |
### 23.1.6 ospf

**router-mode**

Enables OSPF routing on a profile or device

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

ospf enable

**Parameters**
- ospf enable

<table>
<thead>
<tr>
<th>ospf enable</th>
<th>Enables OSPF routing on devices using this profile. This option is disabled by default.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#ospf enable
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
  router ospf
    ospf enable
    network 1.2.3.0/24 area 4.5.6.7
    area 0.0.0.4
    auto-cost reference-bandwidth 1
    default-information originate metric 1 metric-type 2
    ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

**Related Commands**

| no | Disables OSPF routing on a profile or device |
23.1.7 passive

`router-mode`

Configures specified OSPF interface as passive. This option is disabled by default.

A passive interface receives routing updates, but does not transmit them.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

```
passive [WORD] | all | vlan <1-4094>
```

**Parameters**

- `passive [WORD] | all | vlan <1-4094>`

<table>
<thead>
<tr>
<th><code>&lt;WORD&gt;</code></th>
<th>Enables the OSPF passive mode on the interface specified by the <code>&lt;WORD&gt;</code> parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Enables the OSPF passive mode on all the L3 interfaces</td>
</tr>
<tr>
<td><strong>vlan &lt;1-4094&gt;</strong></td>
<td>Enables the OSPF passive mode on the specified VLAN interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-4094&gt;</code> — Specify the VLAN interface ID from 1 - 4094.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#passive vlan 1
```

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  passive vlan1
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

**Related Commands**

- `no` Disables the OSPF passive mode on a specified interface
### 23.1.8 redistribute

#### router-mode

Specifies the route types redistributed by OSPF

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

#### Syntax

redistribute [bgp|connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}

#### Parameters

- redistribute [connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Redistributes all BGP routes by OSPF</td>
</tr>
<tr>
<td>connected</td>
<td>Redistributes all connected interface routes by OSPF</td>
</tr>
<tr>
<td>kernel</td>
<td>Redistributes all routes that are neither connected, static, dynamic, nor bgp</td>
</tr>
<tr>
<td>static</td>
<td>Redistributes static routes by OSPF</td>
</tr>
<tr>
<td>metric &lt;0-16777214&gt;</td>
<td>The following keywords are common to the ‘bgp’, ‘connected’, ‘kernel’, and ‘static’ parameters:</td>
</tr>
<tr>
<td></td>
<td>• metric &lt;0-16777214&gt; – Optional. Specifies the OSPF metric value for redistributed routes.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-16777214&gt; – Specify a value from 0 - 16777214.</td>
</tr>
<tr>
<td>metric-type [1</td>
<td>2]</td>
</tr>
<tr>
<td></td>
<td>• metric-type [1</td>
</tr>
<tr>
<td></td>
<td>• 1 – Sets the OSPF external type 1 metrics</td>
</tr>
<tr>
<td></td>
<td>• 2 – Sets the OSPF external type 2 metrics</td>
</tr>
</tbody>
</table>

#### Examples

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#redistribute static metric-type 1

rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
router ospf
ospf enable
network 1.2.3.0/24 area 4.5.6.7
area 0.0.0.4
auto-cost reference-bandwidth 1
default-information originate metric 1 metric-type 2
redistribute static metric-type 1
passive vlan1
ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#

#### Related Commands

no Removes the OSPF redistribution of various route types
23.1.9 route-limit

`router-mode`

Limits the number of routes managed by OSPF. The maximum limit supported by the platform is the default configuration defined under the router-ospf context.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

### Syntax

```
route-limit [num-routes|reset-time|retry-count|retry-timeout]
```

```
route-limit [num-routes <DYNAMIC-ROUTE-LIMIT> | reset-time <1-86400> | retry-count <1-32> | retry-timeout <1-3600> ] { (num-routes | reset-time | retry-count | retry-timeout) }
```

### Parameters

- **num-routes**
  - `<DYNAMIC-ROUTE-LIMIT>`
  - Specifies the maximum number of non self-generated LSAs this process can receive
    - `<DYNAMIC-ROUTE-LIMIT>` – Specify the dynamic route limit.

- **reset-time**
  - `<1-86400>`
  - Specifies the time, in seconds, after which the retry-count is reset to zero
    - `<1-86400>` – Specify a value from 1 - 86400 seconds. The default is 360 seconds.

- **retry-count**
  - `<1-32>`
  - Specifies the maximum number of times adjacencies can be suppressed. Each time OSPF gets into an ignore state, a counter increments. If the counter exceeds the timeout configured by the retry-count parameter, OSPF stays in the same ignore state. Manual intervention is required to get OSPF out of the ignore state.
    - `<1-32>` – Specify a value from 1 - 32. The default is 5.

- **retry-timeout**
  - `<1-3600>`
  - Specifies the retry time in seconds. During this time, OSPF remains in ignore state and all adjacencies are suppressed.
    - `<1-3600>` – Specify a value from 1 - 3600 seconds. The default is 60 seconds.

### Examples

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
```

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context
router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
  ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

### Related Commands

- **no**
  - Removes the limit on the number of routes managed by OSPF
### 23.1.10 router-id

**router-mode**

Specifies the OSPF router ID.

This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

**Syntax**

```
router-id <IP>
```

**Parameters**

- `router-id <IP>`

<table>
<thead>
<tr>
<th>&lt;IP&gt;</th>
<th>Identifies the OSPF router by its IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;IP&gt; – Specify the router ID in the IP &lt;A.B.C.D&gt; format</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#router-id 172.16.10.8
```

Reload, or execute "clear ip ospf process" command, for this to take effect

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

**Related Commands**

- `no` Removes the configured OSPF router ID
23.1.11 no

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|route-limit|router-id]

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Negates a command or set its defaults |

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

The following example shows the OSPF router interface settings before the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context router ospf
    network 1.2.3.0/24 area 4.5.6.7
    area 0.0.0.4
    auto-cost reference-bandwidth 1
    default-information originate metric 1 metric-type 2
    redistribute static metric-type 1
    passive vlan1
    route-limit num-routes 10 reset-time 10
    ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

The following example shows the OSPF router interface settings after the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no area 4
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no auto-cost reference-bandwidth
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#no network 1.2.3.0/24 area 4.5.6.7
```

The following example shows the OSPF router interface settings after the 'no' commands are executed:

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context router ospf
    default-information originate metric 1 metric-type 2
    redistribute static metric-type 1
    passive vlan1
    route-limit num-routes 10 reset-time 10
    ip default-gateway priority 1
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```
CHAPTER 24
ROUTING-POLICY

This chapter summarizes routing-policy commands in the CLI command structure.

Routing policies enable network administrators to control data packet routing and forwarding. Policy-based routing (PBR) always overrides protocol-based routing. Network administrators can define routing policies based on parameters, such as access lists, packet size etc. For example, a routing policy can be configured to route packets along user-defined routes.

In addition to the above, PBR facilitates the provisioning of preferential service to specific traffic. PBR minimally provides the following:

- A means to use source address, protocol, application, and traffic class as traffic routing criteria
- A means to load balance multiple WAN uplinks
- A means to selectively mark traffic for Quality of Service (QoS) optimization

Use the (config) instance to configure router-policy commands. To navigate to the (config-routing-policy mode) instance, use the following commands:

```
<DEVICE>(config)#routing-policy <ROUTING-POLICY-NAME>
```

```
rfs7000-37FABE(config)#routing-policy testpolicy
```

Routing Policy Mode commands:

- `apply-to-local-packets`: Use Policy Based Routing for packets generated by the device
- `logging`: Enable logging for this Route Map
- `no`: Negate a command or set its defaults
- `route-map`: Create a Route Map
- `use`: Set setting to use
- `clrscr`: Clears the display screen
- `commit`: Commit all changes made in this session
- `do`: Run commands from Exec mode
- `end`: End current mode and change to EXEC mode
- `exit`: End current mode and down to previous mode
- `help`: Description of the interactive help system
- `revert`: Revert changes
- `service`: Service Commands
- `show`: Show running system information
- `write`: Write running configuration to memory or terminal

```
rfs7000-37FABE(config-routing-policy-testpolicy)#
```
NOTE: The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore `_` character. In other words, the name of a device cannot contain an underscore.
24.1 routing-policy-commands

The following table summarizes routing policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply-to-local-packets</td>
<td>Enables PBR for locally generated packets</td>
<td>page 24-4</td>
</tr>
<tr>
<td>logging</td>
<td>Enables logging for a specified route map</td>
<td>page 24-5</td>
</tr>
<tr>
<td>route-map</td>
<td>Creates a route map entry</td>
<td>page 24-6</td>
</tr>
<tr>
<td>use</td>
<td>Defines default settings to use</td>
<td>page 24-16</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its defaults</td>
<td>page 24-17</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
24.1.1 apply-to-local-packets

**routing-policy-commands**

Enables PBR for locally generated packets (packets generated by the device). When enabled, this option implements the match and action clauses defined within route maps. This option is enabled by default. To disable PBR, use the `no apply-to-local-packets` command.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
apply-to-local-packets
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-routing-policy-testpolicy)#apply-to-local-packets
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables PBR for locally generated packets</td>
</tr>
</tbody>
</table>
24.1.2 logging

Enables logging for a specified route map. When enabled, this option logs events generated by the enforcement of route-maps. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
logging

Parameters
None

Examples
rfs7000-37FABE(config-routing-policy-testpolicy)#logging

rfs7000-37FABE(config-routing-policy-testpolicy)#show context routing-policy testpolicy
logging
rfs7000-37FABE(config-routing-policy-testpolicy)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables route map logging</td>
</tr>
</tbody>
</table>
24.1.3 route-map

- **routing-policy-commands**

  Creates a route map entry and enters the route map configuration mode

In *policy-based routing* (PBR), route maps control the flow of traffic within the network. They override route tables and direct traffic along a specific path.

Route-maps contain a set of filters that select traffic (*match* clauses) and associated actions (*mark* clauses) for routing. Every route-map entry has a precedence value. Lower the precedence, higher is the route-map’s priority. All incoming packets are matched against these route-maps entries. The route-map entry with highest precedence (lowest numerical value) is applied first. In case of a match, action is taken based on the mark clause specified in the route-map. In case of no match, the route-map entry with the next highest precedence is applied. If the incoming packet does not match any of the route-map entries, it is subjected to typical destination-based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- **IP Access List** - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

  ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- **IP DSCP** - Packet filtering can be performed by traffic class, as determined from the IP *Differentiated Services Code Point* (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.

- **Incoming WLAN** - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:

  - **Device with** an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.

  - **Device without** an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.

- **Client role** - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MiNT tunneled packets.

- **Incoming SVI** - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

Mark (or action) clauses determine the routing function when a packet satisfies match criteria. If no mark clauses are defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped. The mark clause defines one of following actions:

- **Next hop** - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used. But if all next hops are unreachable, typical destination-based route lookup is performed.

- **Default next hop** - If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This can be either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the *next hop* and the *default next-hop* is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reversed. In both cases:
  
  a. If a defined next hop is reachable, it is used. If fallback is configured refer to (b).
  
  b. Perform normal destination-based route lookup. If a next hop is found, it is used, if not refer to (c).
  
  c. If default next hop is configured and reachable, it is used, if not, packet is dropped.
• **Fallback** - Enables fallback to destination-based routing if none of the configured next hops are reachable (or not configured). This is enabled by default.

• **Mark IP DSCP** - Configures IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

Supported in the following platforms:

• Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX

• Wireless Controllers — RFS4000, RFS6000, RFS7000

• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
route-map <1-100>
```

Parameters

• `route-map <1-100>` Creates a route map entry, sets a precedence value for the route map, and enters the route map configuration mode

Note: Lower the sequence number, higher is the precedence.

Examples

```
rfs7000-37FABE(config-routing-policy-testpolicy)#route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy)#show context
rout policy testpolicy
  logging
route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

```
rfs7000-37FABE(config-routing-policy-testpolicy)#route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#?
```

Route Map Mode commands:

- `default-next-hop` Default next-hop configuration (aka gateway-of-last-resort)
- `fallback` Fallback to destination based routing if no next-hop is configured or all are unreachable
- `mark` Mark action for route map
- `match` Match clause configuration for Route Map
- `next-hop` Next-hop configuration
- `no` Negate a command or set its defaults

```
clrscr
commit
do
end
exit
help
revert
service
show
write
```

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

```
no
```

Removes a route map
24.1.4 route-map-mode

The following table summarizes route-map configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-next-hop</td>
<td>Sets the default next hop for packets satisfying match criteria</td>
<td>page 24-9</td>
</tr>
<tr>
<td>fallback</td>
<td>Configures a fallback to the next destination</td>
<td>page 24-10</td>
</tr>
<tr>
<td>mark</td>
<td>Marks action clause for packets satisfying match criteria</td>
<td>page 24-11</td>
</tr>
<tr>
<td>match</td>
<td>Sets match clauses for the route map</td>
<td>page 24-12</td>
</tr>
<tr>
<td>next-hop</td>
<td>Sets the next hop for packets satisfying match criteria</td>
<td>page 24-14</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 24-15</td>
</tr>
</tbody>
</table>
24.1.4.1 default-next-hop

 Sets the default next hop for packets satisfying match criteria

 If a packet, subjected to PBR, does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reverse. Use this command to set either the default next hop IP address or define either a WWAN1, PPPoE1, or VLAN interface.

 Supported in the following platforms:

 - Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
 - Wireless Controllers — RFS4000, RFS6000, RFS7000
 - Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

 Syntax

default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]

 Parameters

 - default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]

<table>
<thead>
<tr>
<th>default-next-hop</th>
<th>Sets the next hop router to which packets are sent in case the next hop is not the adjacent router</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>Specifies next hop router’s IP address</td>
</tr>
<tr>
<td>&lt;ROUTER-IF-NAME&gt;</td>
<td>Specifies the outgoing interface name (router interface name)</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Specifies the PPPoE interface</td>
</tr>
<tr>
<td>serial &lt;SLOT-ID&gt;</td>
<td>Specifies the serial interface’s slot, port, and channel group IDs</td>
</tr>
<tr>
<td>&lt;PORT-ID&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;CHANNEL-GROUP-ID&gt;</td>
<td></td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Specifies a VLAN interface ID</td>
</tr>
<tr>
<td>wwan1</td>
<td>Specifies the WAN interface</td>
</tr>
</tbody>
</table>

 Examples

 rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#default-next-hop wwan1
 rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context route-map 1
default-next-hop wwan1
 rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#

 Related Commands

 no | Removes default next hop router settings
24.1.4.2 `fallback`

`route-map-mode`

Enables fallback to destination-based routing. This option is enabled by default. To disable fallback, use the `no fallback` command.

The action taken for packets satisfying the match criteria is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing.

**NOTE:** If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```bash
fallback
```

**Parameters**

None

**Examples**

```bash
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#fallback
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables fallback to destination-based routing, if no next hop is configured or are unreachable</td>
</tr>
</tbody>
</table>
24.1.3 mark

`route-map-mode`

Enables the marking of the DSCP field in the IP header

Use this command to set the IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

The DSCP field in an IP header enables packet classification. Packet filtering can be done based on traffic class, determined from the IP DSCP field. One DSCP value can be configured per route map entry.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
mark ip dscp <0-63>
```

Parameters

- `mark ip dscp <0-63>`

```
<table>
<thead>
<tr>
<th>ip dscp &lt;0-63&gt;</th>
<th>Marks the DSCP field in the IP header</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;0-63&gt; – Specify a DSCP value from 0 - 63.</td>
</tr>
</tbody>
</table>
```

Examples

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
default-next-hop wwan1
route-map 1
mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

```
no
```

Disables marking of IP packets
24.1.4.4 match

route-map-mode

Sets the match clauses

Each route map entry has a set of match clauses used to segregate and filter packets. Packets can be segregated using any one of the following criteria:

- **IP Access List** - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.
  
  ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- **IP DSCP** - Packet filtering can be performed by traffic class, as determined from the IP Differentiated Services Code Point (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.

- **Incoming WLAN** - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:
  
  - **Device with** an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
  
  - **Device without** an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.

- **Client role** - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MiNT tunneled packets.

- **Incoming SVI** - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

The action taken for filtered packets is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. For more information on configuring mark clauses, see `mark`. And for more information on fallback action, see `fallback`.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
match [incoming-interface|ip|ip-access-list|wireless-client-role|wlan]
match incoming-interface [<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]
match ip dscp <0-63>
macth ip-access-list <IP-ACCESS-LIST-NAME>
macth wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>
macth wlan <WLAN-NAME>
```

Parameters

- `match incoming-interface [<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]`

<table>
<thead>
<tr>
<th>incoming-interface</th>
<th>Sets the incoming SVI match clause. Specify an interface name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ROUTER-IF-NAME&gt;</td>
<td>Specifies the layer 3 interface name (route interface)</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Specifies the PPP over Ethernet interface</td>
</tr>
<tr>
<td>Serial Interface</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>serial &lt;SLOT-ID&gt; &lt;PORT-ID&gt; &lt;CHANNEL-GROUP-ID&gt;</code></td>
<td>Specifies the serial interface’s slot, port, and channel group IDs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan &lt;1-4094&gt;</code></td>
<td>Specifies the VLAN interface</td>
</tr>
<tr>
<td>- <code>&lt;1-4094&gt;</code> – Specify a VLAN ID from 1 - 4094.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WAN Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wwan1</code></td>
<td>Specifies the WAN interface name</td>
</tr>
</tbody>
</table>

- **match ip dscp <0-63>**

<table>
<thead>
<tr>
<th>DSCP Match Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dscp &lt;0-63&gt;</code></td>
<td>Sets the DSCP match clause</td>
</tr>
<tr>
<td>- <code>&lt;0-63&gt;</code> – Specify a value from 0 - 63. The defined DSCP value is used as a matching clause for this route map.</td>
<td></td>
</tr>
</tbody>
</table>

- **match ip-access-list <IP-ACCESS-LIST-NAME>**

<table>
<thead>
<tr>
<th>IP Access List Match Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-access-list &lt;IP-ACCESS-LIST-NAME&gt;</code></td>
<td>Sets the match clause using a pre-configured IP access list</td>
</tr>
<tr>
<td>- <code>&lt;IP-ACCESS-LIST-NAME&gt;</code> – Specify a pre-configured IP access list name.</td>
<td></td>
</tr>
</tbody>
</table>

- **match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>**

<table>
<thead>
<tr>
<th>Wireless Client Role Match Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wireless-client-role &lt;ROLE-POLICY-NAME&gt; &lt;ROLE-NAME&gt;</code></td>
<td>Sets the wireless client role match clause</td>
</tr>
<tr>
<td>- <code>&lt;ROLE-POLICY-NAME&gt;</code> – Specify a pre-configured role policy</td>
<td></td>
</tr>
<tr>
<td>- <code>&lt;ROLE-NAME&gt;</code> – Specify a pre-configured role within the specified role policy.</td>
<td></td>
</tr>
</tbody>
</table>

- **match wlan <WLAN-NAME>**

<table>
<thead>
<tr>
<th>WLAN Match Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wlan &lt;WLAN-NAME&gt;</code></td>
<td>Sets the incoming WLAN match clause. Specify a WLAN name.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#match incoming-interface pppoe1
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context route-map 1
  match incoming-interface pppoe1
  default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

**Related Commands**

- **no** Disables match clause settings for this route map
24.1.4.5 next-hop

*route-map-mode*

Sets the next hop for packets satisfying match criteria

This command allows you to configure the primary and secondary hop priority requests.

Define the primary and secondary hop settings. When defined, the primary hop resource is used with no additional
considerations when ever it is available.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
```

Parameters

- `next-hop` 
  - `<IP>` | `<ROUTER-IF-NAME>` | `pppoel` | `serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>` | `vlan <1-4094>` | `wwlan1`

  Specifies the primary and secondary next hop router’s IP address

- `<WORD>`
  - Specifies the layer 3 Interface name (router interface)

- `pppoel`
  - Specifies the PPP over Ethernet interface

- `serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>`
  - Specifies the serial interface’s slot, port, and channel group IDs.

- `vlan <1-4094>`
  - Specifies the VLAN interface

- `wwan1`
  - Specifies the WAN interface

Examples

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#next-hop vlan 1
```

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
  match incoming-interface pppoe1
  next-hop vlan1
  default-next-hop wwan1
  mark ip dscp 7
```

Related Commands

*no*

Disables the next hop router settings
24.1.4.6 no

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
no [default-next-hop|fallback|mark|match|next-hop]
```

Parameters

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Negates a command or set its defaults</th>
</tr>
</thead>
</table>

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

The following example shows the route-map ‘1’ settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
  match incoming-interface pppoe1
  next-hop vlan1
  default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#no default-next-hop
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#no next-hop
```

The following example shows the route-map ‘1’ settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
  match incoming-interface pppoe1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```
24.1.5 use

routing-policy-commands

Uses Critical Resource Management (CRM) to monitor link status

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

use critical-resource-monitoring

Parameters

- use critical-resource-monitoring

| use critical-resource-monitoring | Uses CRM to monitor the status of a link. Selecting this option determines the disposition of the route-map next hop via monitored critical resources. Link monitoring is the function used to determine a potential fail over to the secondary next hop. This option is enabled by default. |

Examples

rfs7000-37FABE(config-routing-policy-testpolicy)#use critical-resource-monitoring
rfs7000-37FABE(config-routing-policy-testpolicy)#

Related Commands

- no | Disables CRM link status monitoring |
### 24.1.6 no

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
no [apply-to-local-packets|logging|route-map|use]
```

#### Parameters

- `no <PARAMETERS>`

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Negates a command or set its defaults</th>
</tr>
</thead>
</table>

#### Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

#### Examples

The following example shows the routing policy ‘testpolicy’ settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
  logging
    route-map 1
      match incoming-interface pppoe1
        default-next-hop wwan1  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy)#
```

```
rfs7000-37FABE(config-routing-policy-testpolicy)#no logging
rfs7000-37FABE(config-routing-policy-testpolicy)#no route-map 1
rfs7000-37FABE(config-routing-policy-testpolicy)#no apply-to-local-packets
```

The following example shows the routing policy ‘testpolicy’ settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
  no apply-to-local-packets
rfs7000-37FABE(config-routing-policy-testpolicy)#
```
CHAPTER 25
AAA-TACACS-POLICY

This chapter summarizes the accounting, authentication, and authorization (AAA) Terminal Access Control Access-Control System (TACACS) policy commands in the CLI command structure.

TACACS is a network security application that provides additional network security by providing a centralized authentication, authorization, and accounting platform. TACACS implementation requires configuration of the TACACS authentication server and database.

Use the (config) instance to configure AAA-TACACS policy commands. To navigate to the config-aaa-tacacs-policy instance, use the following commands:

```plaintext
<DEVICE>(config)#aaa-tacacs-policy <POLICY-NAME>
```

```plaintext
rfs7000-37FABE(config)#aaa-tacacs-policy test
rfs7000-37FABE(config-aaa-tacacs-policy-test)#?
```

AAA TACACS Policy Mode commands:
- **accounting** Configure accounting parameters
- **authentication** Configure authentication parameters
- **authorization** Configure authorization parameters
- **no** Negate a command or set its defaults
- **clrscr** Clears the display screen
- **commit** Commit all changes made in this session
- **do** Run commands from Exec mode
- **end** End current mode and change to EXEC mode
- **exit** End current mode and down to previous mode
- **help** Description of the interactive help system
- **revert** Revert changes
- **service** Service Commands
- **show** Show running system information
- **write** Write running configuration to memory or terminal

```plaintext
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
25.1 aaa-tacacs-policy

The following table summarizes AAA-TACACS policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Configures TACACS accounting parameters</td>
<td>page 25-3</td>
</tr>
<tr>
<td>authentication</td>
<td>Configures TACACS authentication parameters</td>
<td>page 25-6</td>
</tr>
<tr>
<td>authorization</td>
<td>Configures TACACS authorization parameters</td>
<td>page 25-9</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 25-12</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
### 25.1.1 accounting

> **aaa-tacacs-policy**

Configures the server type and interval at which interim accounting updates are sent to the server. Up to 2 accounting servers can be configured.

This feature tracks user activities on the network, and provides information such as, resources used and usage time. This information can be used for audit and billing purposes.

TACACS accounting tracks user activity and is useful for security audit purposes.

**Supported in the following platforms:**
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

accounting [access-method|auth-fail|commands|server|session]

accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}

accounting [auth-fail|commands|session]

accounting server [<1-2>|preference]

accounting server preference [authenticated-server-host|authenticated-server-number|authorized-server-host|authorized-server-number|none]

accounting server <1-2> [host|retry-timeout-factor <50-200>|timeout]

accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]}

accounting server <1-2> port <1-65535>

accounting server <1-2> timeout <3-5> {attempts <1-3>}

**Parameters**

- **access-method**
  - **all** Configures TACACS accounting for all access modes
  - **console** Configures TACACS accounting for console access only
  - **ssh** Configures TACACS accounting for SSH access only
  - **telnet** Configures TACACS accounting for Telnet access only

- **auth-fail** Enables accounting for authentication fail details. This option is disabled by default.

- **commands** Enables accounting of commands executed. This option is disabled by default.

- **session** Enables accounting for session start and stop details. This option is disabled by default.

- **server** Configures a TACACS accounting server
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>preference</td>
<td>Configures the accounting server preference (specifies the method of selecting a server, from the pool, to send the request)</td>
</tr>
<tr>
<td>authenticated-server-host</td>
<td>Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is referred to by its hostname.</td>
</tr>
<tr>
<td>authenticated-server-number</td>
<td>Sets the authentication server as the accounting server This parameter indicates the same server is used for authentication and accounting. The server is referred to by its index or number.</td>
</tr>
<tr>
<td>authorized-server-host</td>
<td>Sets the authorization server as the accounting server This parameter indicates the same server is used for authorization and accounting. The server is referred to by its hostname.</td>
</tr>
<tr>
<td>authorized-server-number</td>
<td>Sets the authorized server as the accounting server This parameter indicates the same server is used for authorization and accounting. The server is referred to by its index number.</td>
</tr>
<tr>
<td>none</td>
<td>Indicates the accounting server is independent of the authentication and authorization servers</td>
</tr>
</tbody>
</table>

- accounting server <1-2> retry-timeout-factor <50-200>

<table>
<thead>
<tr>
<th>server &lt;1-2&gt;</th>
<th>Configures an accounting server. Up to 2 accounting servers can be configured</th>
</tr>
</thead>
</table>
| retry-timeout-factor <50-200> | Sets the scaling factor for retry timeouts  
  • <50-200> – Specify a value from 50 - 200. The default is 100.  
  A value of 100 indicates the time gap between two consecutive retries remains the same irrespective of the number of retries.  
  A value lesser than 100 indicates the time gap between two consecutive retries reduces with each successive retry.  
  A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry. |

- accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}

<table>
<thead>
<tr>
<th>server &lt;1-2&gt;</th>
<th>Configures an accounting server. Up to 2 accounting servers can be configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Configures the accounting server’s IP address or hostname</td>
</tr>
</tbody>
</table>
| secret [0 <SECRET>|2 <SECRET>|<SECRET>] | Optional. Configures a common secret key used to authenticate with the accounting server  
  • 0 <SECRET> – Configures a clear text secret key  
  • 2 <SECRET> – Configures an encrypted secret key  
  • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters. |
| port <1-65535> | Optional. Configures the accounting server port (the port used to connect to the accounting server)  
  • <1-65535> – Specify the TCP accounting port number from 1 - 65535. The default port is 49. |

- accounting server <1-2> timeout <3-5> {attempts <1-3>}

| server <1-2>          | Configures an accounting server. Up to 2 accounting servers can be configured                           |
timeout <3-5>  Configures the timeout for each request sent to the TACACS accounting server. This is the time allowed to elapse before another request is sent to the TACACS accounting server. If a response is received from the server within this time, no retry is attempted.
   • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.

attempts <1-3>  Optional. Specifies the number of times a transmission request is attempted. This is the maximum number of times a request is sent to the TACACS accounting server before getting discarded.
   • <1-3> – Specify a value from 1 - 3. The default is 3.

Examples
rfs7000-37FABE(config-aaa-tacacs-policy-test)#accounting auth-fail
rfs7000-37FABE(config-aaa-tacacs-policy-test)#accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#accounting server preference authorized-server-number
rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context aaa-tacacs-policy test
   accounting server preference authorized-server-number
   accounting auth-fail
   accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#

Related Commands

no  Resets values or disables commands
25.1.2 authentication

aaa-tacacs-policy

Configures user authentication parameters. Users are allowed or denied access to the network based on the authentication parameters set.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

authentication [access-method|directed-request|server|service]

access-method Configures access modes for TACACS authentication. The options are: console, SSH, Telnet, Web, and all.

all Authenticates users using all access modes (console, SSH, and Telnet)

console Authenticates users using console access only

ssh Authenticates users using SSH access only

telnet Authenticates users using Telnet access only

web Authenticates users using Web interface only

directed-request Enables user to specify TACACS server to use with `@server'. This option is disabled by default.

Note: The specified server should be present in the configured servers list.

server <1-2> Configures a TACACS authentication server. Up to 2 TACACS servers can be configured

- <1-2> – Specify the TACACS server index from 1 - 2.

host <IP/HOSTNAME> Sets the TACACS server’s IP address or hostname

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-method [all</td>
<td>console</td>
</tr>
<tr>
<td>directed-request</td>
<td>Enables user to specify TACACS server to use with `@server'. This option is disabled by default.</td>
</tr>
<tr>
<td>server &lt;1-2&gt; host &lt;IP/HOSTNAME&gt; {secret [0 &lt;SECRET&gt;</td>
<td>2 &lt;SECRET&gt;</td>
</tr>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Sets the TACACS server’s IP address or hostname</td>
</tr>
</tbody>
</table>
### AAA-TACACS-POLICY 25-7

| Secret [0 <SECRET>, 2 <SECRET>, <SECRET>] | Configures the secret key used to authenticate with the TACACS server  
| • 0 <SECRET> – Configures a clear text secret  
| • 2 <SECRET> – Configures an encrypted secret  
| • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters. |
| Port <1-65535> | Optional. Specifies the port used to connect to the TACACS server  
| • <1-65535> – Specify a value for the TCP authentication port from 1 - 65535. The default port is 49. |
| Server <1-2> | Configures a TACACS authentication server. Up to 2 TACACS servers can be configured  
| • <1-2> – Specify the TACACS server index from 1 - 2. |
| Retry-timeout-factor <50-200> | Configures timeout scaling between two consecutive TACACS authentication retries  
| • <50-200> – Specify the scaling factor from 50 - 200. The default is 100.  
| A value of 100 indicates the interval between consecutive retries remains the same irrespective of the number of retries.  
| A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry.  
| A value greater than 100 indicates the interval between consecutive retries increases with each successive retry. |
| Server <1-2> | Configures a TACACS authentication server. Up to 2 TACACS servers can be configured  
| • <1-2> – Specify the TACACS server index from 1-2. |
| Timeout <3-60> | Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted.  
| • <3-60> – Specify a value from 3-60 seconds. The default is 3 seconds. |
| Attempts <1-10> | Optional. Indicates the number of retry attempts to make before giving up  
| • <1-10> – Specify a value from 1-10. The default is 3. |
| Authentication service <SERVICE-NAME> {Protocol <AUTHENTICATION-PROTO-NAME>} | Configures the TACACS authentication service name  
| Protocol <AUTHENTICATION-PROTO-NAME> | Optional. Specify the authentication protocol used with this TACACS policy.  
| Note: A maximum of five entries is allowed. |
Examples

rfs7000-37FABE(config-aaa-tacacs-policy-test)#authentication directed-request

rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
  authentication directed-request
  accounting server preference authorized-server-number
  accounting auth-fail
  accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#

Related Commands

| no          | Resets values or disables commands |
25.1.3 authorization

- aaa-tacacs-policy

Configures authorization parameters

This feature allows network administrators to limit user accessibility and configure varying levels of accessibility for different users.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

authorization [access-method|allow-privileged-commands|server]

authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}

authorization server [<1-2>|preference]

authorization server <1-2> [host|retry-timeout-factor|timeout]

authorization server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]}

authorization server <1-2> port <1-65535>

authorization server <1-2> retry-timeout-factor <50-200>

authorization server <1-2> timeout <3-5> {attempts <1-3>}

authorization server preference [authenticated-server-host|authenticated-server-number|none]

Parameters

- authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}

<table>
<thead>
<tr>
<th>access-method</th>
<th>Configures the access method for command authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Authorizes commands from all access methods</td>
</tr>
<tr>
<td>console</td>
<td>Authorizes commands from the console only</td>
</tr>
<tr>
<td>telnet</td>
<td>Authorizes commands from Telnet only</td>
</tr>
<tr>
<td>ssh</td>
<td>Authorizes commands from SSH only</td>
</tr>
<tr>
<td>{console</td>
<td>ssh</td>
</tr>
</tbody>
</table>

- authorization allow-privileged-commands

<table>
<thead>
<tr>
<th>allow-privileged-commands</th>
<th>Allows privileged commands execution without command authorization. This option is disabled by default.</th>
</tr>
</thead>
</table>

- authorization server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]}

<table>
<thead>
<tr>
<th>server &lt;1-2&gt;</th>
<th>Configures a TACACS authorization server. Up to 2 TACACS servers can be configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Sets the TACACS server’s IP address or hostname</td>
</tr>
</tbody>
</table>
### WiNG 5.8.1 CLI Reference Guide

| secret [0 <SECRET>| 2 <SECRET>]<SECRET> | Optional. Configures the secret used to authorize with the TACACS server  
|  | - 0 <SECRET> – Configures a clear text secret  
|  | - 2 <SECRET> – Configures an encrypted secret  
|  | - <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.  
| port <1-65535> | Optional. Specifies the port used to connect to the TACACS server  
|  | - <1-65535> – Specify a value for the TCP authorization port from 1 - 65535. The default port is 49.  
| preference | Configures the authorization server preference  
| authenticated-server-host | Sets the authentication server as the authorization server  
|  | This parameter indicates the same server is used for authentication and authorization. The server is referred to by its hostname.  
| authenticated-server-number | Sets the authentication server as the authorization server  
|  | This parameter indicates the same server is used for authentication and authorization. The server is referred to by its index or number.  
| none | Indicates the authorization server is independent of the authentication
Examples
rfs7000-37FABE(config-aaa-tacacs-policy-test)#authorization allow-privileged-commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
  authentication directed-request
  accounting server preference authorized-server-number
  authorization allow-privileged-commands
  accounting auth-fail
  accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#

Related Commands

| no      | Resets values or disables commands |
25.1.4 **no**

Negates a AAA TACACS policy command or sets its default

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [accounting|authentication|authorization]

**Parameters**

- no <PARAMETERS>

<table>
<thead>
<tr>
<th>no &lt;PARAMETERS&gt;</th>
<th>Provide the parameters needed to reset or disable the desired AAA-TACACS policy setting.</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the AAA-TACACS policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
  authentication directed-request
  accounting server preference authorized-server-number
  authorization allow-privileged-commands
  accounting auth-fail
  accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#no authentication directed-request
rfs7000-37FABE(config-aaa-tacacs-policy-test)#no accounting auth-fail
rfs7000-37FABE(config-aaa-tacacs-policy-test)#no authorization allow-privileged-commands
```

The following example shows the AAA-TACACS policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
  accounting server preference authorized-server-number
  accounting commands
rfs7000-37FABE(config-aaa-tacacs-policy-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>accounting</th>
<th>Configures TACACS accounting parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Configures TACACS authentication parameters</td>
</tr>
<tr>
<td>authorization</td>
<td>Configures TACACS authorization parameters</td>
</tr>
</tbody>
</table>
This chapter summarizes the Meshpoint commands in the CLI command structure. Meshpoints are detector radios that monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

This chapter is organized as follows:

- `meshpoint-config-instance`
- `meshpoint-qos-policy-config-instance`
- `meshpoint-device-config-instance`

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
26.1 meshpoint-config-instance

MeshConnex (MCX) is a mesh networking technology that is comparable to the 802.11s mesh networking specification. MCX meshing uses a hybrid proactive/on-demand path selection protocol, similar to Ad hoc On Demand Distance Vector (AODV) routing protocols. This allows it to form efficient paths using multiple attachment points to a distribution WAN, or form purely ad-hoc peer-to-peer mesh networks in the absence of a WAN. Each device in the MCX mesh proactively manages its own path to the distribution WAN, but can also form peer-to-peer paths on demand to improve forwarding efficiency.

MCX is not compatible with MiNT Based meshing, though the two technologies can be enabled simultaneously in certain circumstances.

MCX is designed for large-scale, high-mobility outdoor mesh deployments. MCX continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MCX uses this data to dynamically form and continually maintain paths for forwarding network frames.

In MCX systems, a meshpoint (MP) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols will continually select the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID. The MeshID is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

Use the (config) instance to configure a meshpoint. To navigate to the meshpoint configuration instance, use the following command:

```
<DEVICE>(config)#meshpoint <MESHPOINT-NAME>
```

```
rfs7000-37FABE(config)#meshpoint test
rfs7000-37FABE(config-meshpoint-test)#?
```

Mesh Point Mode commands:

- `allowed-vlans` Set the allowed VLANs
- `beacon-format` The beacon format of this meshpoint
- `control-vlan` VLAN for meshpoint control traffic
- `data-rates` Specify the 802.11 rates to be supported on this meshpoint
- `description` Configure a description of the usage of this meshpoint
- `force` Force suboptimal paths
- `meshid` Configure the Service Set Identifier for this meshpoint
- `neighbor` Configure neighbor specific parameters
- `no` Negate a command or set its defaults
- `root` Set this meshpoint as root
- `security-mode` The security mode of this meshpoint
- `shutdown` Shutdown this meshpoint
- `use` Set setting to use
- `wpa2` Modify ccmp wpa2 related parameters

```
clrscr
commit
do
end
exit
help
revert
service
show
write
```

```
rfs7000-37FABE(config-meshpoint-test)#
```
The following table summarizes meshpoint configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowed-vlans</td>
<td>Configures VLANs allowed on the meshpoint</td>
<td>page 26-4</td>
</tr>
<tr>
<td>beacon-format</td>
<td>Configures the beacon format for the meshpoint AP</td>
<td>page 26-5</td>
</tr>
<tr>
<td>control-vlan</td>
<td>Configures the VLAN where meshpoint control traffic traverses</td>
<td>page 26-6</td>
</tr>
<tr>
<td>data-rates</td>
<td>Configures the data rates supported per frequency band</td>
<td>page 26-7</td>
</tr>
<tr>
<td>description</td>
<td>Configures a human friendly description for this meshpoint</td>
<td>page 26-11</td>
</tr>
<tr>
<td>force</td>
<td>Forces formation of sub-optimal paths through the meshpoint's root node</td>
<td>page 26-12</td>
</tr>
<tr>
<td>meshid</td>
<td>Configures a unique ID for this meshpoint</td>
<td>page 26-13</td>
</tr>
<tr>
<td>neighbor</td>
<td>Configures the neighbor inactivity time out for this meshpoint</td>
<td>page 26-14</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 26-15</td>
</tr>
<tr>
<td>root</td>
<td>Configures a meshpoint as the root meshpoint</td>
<td>page 26-17</td>
</tr>
<tr>
<td>security-mode</td>
<td>Configures the security mode on the meshpoint.</td>
<td>page 26-19</td>
</tr>
<tr>
<td>service</td>
<td>Allows only 802.11n capable neighbors to create a mesh connection</td>
<td>page 26-21</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the meshpoint</td>
<td>page 26-22</td>
</tr>
<tr>
<td>use</td>
<td>Configures a QoS policy for use with this meshpoint</td>
<td>page 26-23</td>
</tr>
<tr>
<td>wpa2</td>
<td>Configures WPA2 encryption settings</td>
<td>page 26-24</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
26.1.1 allowed-vlans

meshpoint-config-instance

Defines VLANs allowed on the mesh network. A VLAN must be added to the allowed VLANs list for data to be allowed across the mesh network. Use this command to remove VLANs from the list of allowed VLANs.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
allowed-vlans [<VLAN-ID>|add <VLAN-ID>|remove <VLAN-ID>]
```

Parameters

- **allowed-vlans** [<VLAN-ID>|add <VLAN-ID>|remove <VLAN-ID>]
  - Defines VLANs allowed access on the mesh network

| <VLAN-ID> | The VLAN ID or the range of IDs to be managed. A single VLAN or multiple VLANs can be added to the list of allowed VLANs. When adding multiple VLANs, specify the range (for example, 10-20, 25, 30-35). Use this command to create a VLAN list on a new meshpoint. |
| add <VLAN-ID> | Adds a single VLAN or a range of VLANs to the list of allowed VLANs. To specify a range of VLANs, specify the first and last VLAN ID in the range separated by a hyphen (for example, 1-10). |
| remove <VLAN-ID> | Removes a single VLAN or a range of VLANs from the list of allowed VLANs |

Examples

```
rfs7000-37FABE(config-meshpoint-test)#allowed-vlans 1
```

```
rfs7000-37FABE(config-meshpoint-test)#allowed-vlans add 10-23
```

```
rfs7000-37FABE(config-meshpoint-test)#allowed-vlans remove 17
```

```
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
  meshid test
  beacon-format mesh-point
  control-vlan 1
  allowed-vlans 1,10-16,18-23
  security-mode none
  no root
```

Related Commands

| no | Clears the list of VLANs allowed access to the mesh network |
26.1.2 beacon-format

meshpoint-config-instance

Configures the beacon transmission format for this meshpoint. Beacons are transmitted periodically to advertise that a wireless network is available. It contains all the required information for a device to connect to the network. The beacon format advertises how a mesh capable AP71XX acts. APs can act either as an access point or a meshpoint.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

beacon-format [access-point|mesh-point]

Parameters

- beacon-format [access-point|mesh-point]

<table>
<thead>
<tr>
<th>beacon-format</th>
<th>Configures how a mesh capable AP71XX acts in a mesh network</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-point</td>
<td>Uses access point style beacons</td>
</tr>
<tr>
<td>mesh-point</td>
<td>Uses meshpoint style beacons (this is the default setting)</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-meshpoint-test)#beacon-format mesh-point

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
meshid test
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
security-mode none
no root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands

- no | Resets the beacon format for this meshpoint to its default (mesh-point) |
26.1.3 control-vlan

meshpoint-config-instance

Configures a VLAN as the dedicated control VLAN.

Mesh management traffic can be sent over a dedicated VLAN. This dedicated VLAN is known as a control VLAN, and should be configured in the backhaul port of all the access points configured as meshpoint roots. Once configured, the control VLAN enables communication between meshpoint’s root APs.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

control-vlan <1-4094>

Parameters

- control-vlan <1-4094>

<table>
<thead>
<tr>
<th>control-vlan &lt;1-4094&gt;</th>
<th>Configures a VLAN as a dedicated carrier of mesh management traffic</th>
</tr>
</thead>
</table>
| control-vlan <1-4094> | Configures the control VLAN
  • <1-4094> – Specify the control VLAN from 1 - 4094. The default is VLAN 1.
  **Note:** If VLAN 1 is configured as the control VLAN, ensure that the VLAN is configured in the wired port of all access points belonging to same meshpoint.
  **Note:** Control VLAN need not necessarily be added in the allowed VLAN list.

Examples

rfs7000-37FABE(config-meshpoint-test)#control-vlan 1
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
meshid test
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
security-mode none
no root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands

- control-vlan no
  Resets the control VLAN for this meshpoint to its default of 1
26.1.4 data-rates

meshpoint-config-instance

Configures individual data rates for the 2.4 GHz and 5.0 GHz frequency bands

NOTE: Ensure that the basic data rates configured on a meshpoint's root and non-root access points is the same.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

data-rates [2.4GHz|5GHz]

data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]

data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|
|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)

data-rates 5GHz [a-only|an|default]

data-rates 5GHz custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|
|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|
|mcs0-7|mcs8-15|basic-mcs0-7)

Parameters

- data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]

<table>
<thead>
<tr>
<th>data-rates 2.4GHz</th>
<th>Configures preset data rates for the 2.4 GHz frequency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b-only</td>
<td>Configures data rate for the meshpoint using 802.11b only rates.</td>
</tr>
<tr>
<td>bg</td>
<td>Configures data rate for the meshpoint using 802.11b and 802.11g rates.</td>
</tr>
<tr>
<td>default</td>
<td>Configures data rate for the meshpoint at a pre-configured default rate for this frequency.</td>
</tr>
<tr>
<td>g-only</td>
<td>Configures data rate for the meshpoint using 802.11g only rates.</td>
</tr>
<tr>
<td>gn</td>
<td>Configures data rate for the meshpoint using 802.11g and 802.11n rates.</td>
</tr>
</tbody>
</table>

- data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|
|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)

data-rates 2.4GHz Configures the preset data rates for the 2.4 GHz frequency

Define both minimum Basic and optimal Supported rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band. These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a supported MCS index. Set a Modulation and Coding Scheme (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types.

Contd..
Meshpoints can communicate as long as they support the same basic MCS (as well as non-802.11n basic rates). The selected rates apply to associated client traffic within this mesh point only.

| custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7) |
|---------|---------------------------------|
| Configures custom rates |
| • 1 – Configures the available rate at 1 Mbps |
| • 2 – Configures the available rate at 2 Mbps |
| • 5.5 – Configures the available rate at 5.5 Mbps |
| • 6 – Configures the available rate at 6 Mbps |
| • 9 – Configures the available rate at 9 Mbps |
| • 11 – Configures the available rate at 11 Mbps |
| • 12 – Configures the available rate at 12 Mbps |
| • 18 – Configures the available rate at 18 Mbps |
| • 24 – Configures the available rate at 24 Mbps |
| • 36 – Configures the available rate at 36 Mbps |
| • 48 – Configures the available rate at 48 Mbps |
| • 54 – Configures the available rate at 54 Mbps |
| • basic-1 – Configures the available rate at a basic rate of 1 Mbps |
| • basic-2 – Configures the available rate at a basic rate of 2 Mbps |
| • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps |
| • basic-6 – Configures the available rate at a basic rate of 6 Mbps |
| • basic-9 – Configures the available rate at a basic rate of 9 Mbps |
| • basic-11 – Configures the available rate at a basic rate of 11 Mbps |
| • basic-12 – Configures the available rate at a basic rate of 12 Mbps |
| • basic-18 – Configures the available rate at a basic rate of 18 Mbps |
| • basic-24 – Configures the available rate at a basic rate of 24 Mbps |
| • basic-36 – Configures the available rate at a basic rate of 36 Mbps |
| • basic-48 – Configures the available rate at a basic rate of 48 Mbps |
| • basic-54 – Configures the available rate at a basic rate of 54 Mbps |
| • basic-mcs0-7 – Configures the MCS index range of 0 - 7 for basic rate |
| • mcs0-7 – Configures the MCS index range of 0-7 as the data rate |
| • mcs0-15 – Configures the MCS index range of 0-15 as the data rate |
| • mcs8-15 – Configures the MCS index range of 8-15 as the data rate |

**Note:** Multiple choices can be made from the above list of rates.

| data-rates 5GHz [a-only|an|default] |
|--------------------------------------|
| data-rates 5GHz | Configures the preset data rates for the 5.0 GHz frequency |
| a-only | Configures the data rate for the meshpoint using 802.11a only rates |
| bn | Configures the data rate for the meshpoint using 802.11a and 802.11n rates |
| default | Configures the data rate for the meshpoint at a pre-configured default rate for this frequency |
| g-only | Configures the data rate for the meshpoint using 802.11g only rates |
| gn | Configures the data rate for the meshpoint using 802.11g and 802.11n rates |
- **data-rates 5GHz**

  **Custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)

  **data-rates 5GHz**

  Configures the preset data rates for the 5.0 GHz frequency.

  Define both minimum Basic and optimal Supported rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point.

  If supporting 802.11n, select a supported MCS index. Set a MCS in respect to the radio’s channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-802.11n basic rates). The selected rates apply to associated client traffic within this mesh point only.

| custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7) | Configures custom rates:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6 – Configures the available rate at 6 Mbps</td>
<td>6 – Configures the available rate at 6 Mbps</td>
</tr>
<tr>
<td>9 – Configures the available rate at 9 Mbps</td>
<td>9 – Configures the available rate at 9 Mbps</td>
</tr>
<tr>
<td>12 – Configures the available rate at 12 Mbps</td>
<td>12 – Configures the available rate at 12 Mbps</td>
</tr>
<tr>
<td>18 – Configures the available rate at 18 Mbps</td>
<td>18 – Configures the available rate at 18 Mbps</td>
</tr>
<tr>
<td>24 – Configures the available rate at 24 Mbps</td>
<td>24 – Configures the available rate at 24 Mbps</td>
</tr>
<tr>
<td>36 – Configures the available rate at 36 Mbps</td>
<td>36 – Configures the available rate at 36 Mbps</td>
</tr>
<tr>
<td>48 – Configures the available rate at 48 Mbps</td>
<td>48 – Configures the available rate at 48 Mbps</td>
</tr>
<tr>
<td>54 – Configures the available rate at 54 Mbps</td>
<td>54 – Configures the available rate at 54 Mbps</td>
</tr>
<tr>
<td>basic-1 – Configures the available rate at a basic rate of 1 Mbps</td>
<td>basic-1 – Configures the available rate at a basic rate of 1 Mbps</td>
</tr>
<tr>
<td>basic-2 – Configures the available rate at a basic rate of 2 Mbps</td>
<td>basic-2 – Configures the available rate at a basic rate of 2 Mbps</td>
</tr>
<tr>
<td>basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps</td>
<td>basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps</td>
</tr>
<tr>
<td>basic-6 – Configures the available rate at a basic rate of 6 Mbps</td>
<td>basic-6 – Configures the available rate at a basic rate of 6 Mbps</td>
</tr>
<tr>
<td>basic-9 – Configures the available rate at a basic rate of 9 Mbps</td>
<td>basic-9 – Configures the available rate at a basic rate of 9 Mbps</td>
</tr>
<tr>
<td>basic-11 – Configures the available rate at a basic rate of 11 Mbps</td>
<td>basic-11 – Configures the available rate at a basic rate of 11 Mbps</td>
</tr>
<tr>
<td>basic-12 – Configures the available rate at a basic rate of 12 Mbps</td>
<td>basic-12 – Configures the available rate at a basic rate of 12 Mbps</td>
</tr>
<tr>
<td>basic-18 – Configures the available rate at a basic rate of 18 Mbps</td>
<td>basic-18 – Configures the available rate at a basic rate of 18 Mbps</td>
</tr>
<tr>
<td>basic-24 – Configures the available rate at a basic rate of 24 Mbps</td>
<td>basic-24 – Configures the available rate at a basic rate of 24 Mbps</td>
</tr>
<tr>
<td>basic-36 – Configures the available rate at a basic rate of 36 Mbps</td>
<td>basic-36 – Configures the available rate at a basic rate of 36 Mbps</td>
</tr>
<tr>
<td>basic-48 – Configures the available rate at a basic rate of 48 Mbps</td>
<td>basic-48 – Configures the available rate at a basic rate of 48 Mbps</td>
</tr>
<tr>
<td>basic-54 – Configures the available rate at a basic rate of 54 Mbps</td>
<td>basic-54 – Configures the available rate at a basic rate of 54 Mbps</td>
</tr>
<tr>
<td>basic-mcs0-7 – Configures the MCS index range of 0-7 for basic rate</td>
<td>basic-mcs0-7 – Configures the MCS index range of 0-7 for basic rate</td>
</tr>
<tr>
<td>mcs0-7 – Configures the MCS index range of 0-7 as the data rate</td>
<td>mcs0-7 – Configures the MCS index range of 0-7 as the data rate</td>
</tr>
<tr>
<td>mcs0-15 – Configures the MCS index range of 0-15 as the data rate</td>
<td>mcs0-15 – Configures the MCS index range of 0-15 as the data rate</td>
</tr>
<tr>
<td>mcs8-15 – Configures the MCS index range of 8-15 as the data rate</td>
<td>mcs8-15 – Configures the MCS index range of 8-15 as the data rate</td>
</tr>
</tbody>
</table>

**Note:** Multiple choices can be made from the above list of rates.
Examples

```
rfs7000-37FABE(config-meshpoint-test)#data-rates 2.4GHz bgn
rfs7000-37FABE(config-meshpoint-test)#data-rates 5GHz an
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
  meshid test
  beacon-format mesh-point
  control-vlan 1
  allowed-vlans 1,10-16,18-23
  data-rates 2.4GHz bgn
  data-rates 5GHz an
  security-mode none
  no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets data rates for each frequency band for this meshpoint</td>
</tr>
</tbody>
</table>
26.1.5 description

meshpoint-config-instance

Configures a brief description for this meshpoint. Use this command to describe this meshpoint and its features.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

description <DESCRIPTION>

Parameters
- description <DESCRIPTION>

<table>
<thead>
<tr>
<th>Description</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>description &lt;DESCRIPTION&gt;</td>
<td>Configures a description for this meshpoint</td>
</tr>
<tr>
<td>&lt;DESCRIPTION&gt;</td>
<td>The text describing this meshpoint</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-meshpoint-test)#description "This is an example of a meshpoint description"

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid test
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode none
no root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands

no
Removes the human friendly description provided for this meshpoint
### 26.1.6 force

#### meshpoint-config-instance

Forces formation of sub-optimal paths through the meshpoint's root node. As per legacy behavior, non-root devices under the same root, communicated by forming direct paths through the network. This option allows non-root devices, within the meshpoint, to communicate by forming paths through the root node.

 Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

force peer-paths-through-root

#### Parameters

- **force peer-paths-through-root**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force</td>
<td>Enables formation of sub-optimal paths through the meshpoint root node. This option is disabled by default</td>
</tr>
<tr>
<td>peer-paths-through-root</td>
<td>Enables non-root devices to communicate by forming sub-optimal paths through the root node</td>
</tr>
</tbody>
</table>

#### Examples

```
nx9500-6C8809(config-meshpoint-test)#force peer-paths-through-root
```

```
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
  meshid test
  beacon-format mesh-point
  control-vlan 1
  security-mode none
  no root
  force peer-paths-through-root

nx9500-6C8809(config-meshpoint-test)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables formation of sub-optimal paths through the meshpoint's root node</td>
</tr>
</tbody>
</table>
26.1.7 `meshid`  

meshpoint-config-instance  
Configures a unique Service Set Identifier (SSID) for this meshpoint. This ID is used to uniquely identify this meshpoint.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
meshid <MESH-SSID>
```

Parameters

- `meshid <MESH-SSID>`

Examples

```
rfs7000-37FABE(config-meshpoint-test)#meshid TestingMeshPoint
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode none
no root
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands

```
no
```
Removes the SSID configured for this meshpoint
26.1.8 neighbor

This command configures the inactivity timeout value for neighboring devices. If a frame is not received from the neighbor device for the configured time, then client resources are removed.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
neighbor inactivity-timeout <60-86400>

Parameters
- neighbor inactivity-timeout <60-86400>

Examples
rfs7000-37FABE(config-meshpoint-test)#neighbor inactivity-timeout 300
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
neighbor inactivity-timeout 300
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode none
no root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands
- no
  Removes the configured neighbor inactivity timeout value for this meshpoint
26.1.9 no

meshpoint-config-instance

Negates meshpoint commands or resets their values to default

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [allowed-vlans|beacon-format|control-vlan|description|force|meshid|root|
  security-mode|shutdown]

no data-rates [2.4GHz|5GHz]
no force peer-paths-through-root
no neighbor inactivity-timeout
no use [aaa-policy|meshpoint-qos-policy]

no wpa2 [eap|key-rotation|psk]
no wpa2 eap [auth-type|identity|peap-mschapv2|tls trustpoint]
no wpa2 key-rotation [broadcast|unicast]
no wpa2 psk

no service allow-ht-only

Parameters

- no <PARAMETERS>

| no <PARAMETERS> | Removes or reverts this meshpoint settings to default based on the parameters passed |

Examples

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
shutdown
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
neighbor inactivity-timeout 300
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode psk
wpa2 psk 0 Test Company
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
root
rfs7000-37FABE(config-meshpoint-test)#

rfs7000-37FABE(config-meshpoint-test)#no allowed-vlans
rfs7000-37FABE(config-meshpoint-test)#no beacon-format
rfs7000-37FABE(config-meshpoint-test)#no control-vlan
rfs7000-37FABE(config-meshpoint-test)#no description
rfs7000-37FABE(config-meshpoint-test)#no meshid
rfs7000-37FABE(config-meshpoint-test)#no root
rfs7000-37FABE(config-meshpoint-test)#no security-mode
```plaintext
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
  beacon-format mesh-point
  control-vlan 1
  neighbor inactivity-timeout 300
  data-rates 2.4GHz bgn
  data-rates 5GHz an
  security-mode none
  wpa2 psk 0 Test Company
  wpa2 key-rotation unicast 1200
  wpa2 key-rotation broadcast 600
  no root

rfs7000-37FABE(config-meshpoint-test)#no data-rates 2.4GHz
rfs7000-37FABE(config-meshpoint-test)#no data-rates 5GHz

rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
  beacon-format mesh-point
  control-vlan 1
  neighbor inactivity-timeout 300
  security-mode none
  wpa2 psk 0 Test Company
  wpa2 key-rotation unicast 1200
  wpa2 key-rotation broadcast 600
  no root

nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
  meshid test
  beacon-format mesh-point
  control-vlan 1
  security-mode none
  no root
  force peer-paths-through-root

nx9500-6C8809(config-meshpoint-test)#no force peer-paths-through-root

nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
  meshid test
  beacon-format mesh-point
  control-vlan 1
  security-mode none
  no root
```

26.1.10 root

meshpoint-config-instance

Configures this meshpoint as the root meshpoint. Root meshpoints are generally tied to an Ethernet backhaul for wired connectivity. By default this option is disabled.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

root

Parameters

None

Examples

There are two ways of configuring root access points within a meshpoint.

1. First method:
   - Configure two meshpoints, having the same meshid, one with the root option enabled and the other configured as no root:
     - Apply the root meshpoint to the root access point and the no-root meshpoint to the non-root access points.

   The following examples show the configuration of a meshpoint for the root access point:

   ```
   rfs7000-37FABE(config)#meshpoint root
   rfs7000-37FABE(config-meshpoint-root)#
   rfs7000-37FABE(config-meshpoint-root)#meshid test
   rfs7000-37FABE(config-meshpoint-root)#root
   rfs7000-37FABE(config-meshpoint-root)#security-mode eap
   rfs7000-37FABE(config-meshpoint-root)#commit
   rfs7000-37FABE(config-meshpoint-root)#show context meshpoint test-root
   meshid test
   beacon-format mesh-point
   control-vlan 1
   security-mode eap
   root
   rfs7000-37FABE(config-meshpoint-root)#
   ```

   The following examples show the configuration of a meshpoint for non-root access points:

   ```
   rfs7000-37FABE(config)#meshpoint no-root
   rfs7000-37FABE(config-meshpoint-no-root)#
   rfs7000-37FABE(config-meshpoint-no-root)#meshid test
   rfs7000-37FABE(config-meshpoint-no-root)#security-mode eap
   rfs7000-37FABE(config-meshpoint-no-root)#show context meshpoint no-root
   meshid test
   beacon-format mesh-point
   control-vlan 1
   security-mode eap
   no root
   rfs7000-37FABE(config-meshpoint-no-root)#
   ```
2. Second method:
   - Configure a **no-root** meshpoint and apply to all access points in the meshpoint.
   - Log into the **meshpoint-device > no-root** configuration mode of the **root** access point and **enable root**.

```
rfs7000-37FABE(config-meshpoint-no-root)#show context
meshpoint no-root
  meshid test
  beacon-format mesh-point
  control-vlan 1
  security-mode eap
  no root
rfs7000-37FABE(config-meshpoint-no-root)#
```

```
rfs7000-37FABE(config)#ap81xx B4-C7-99-71-17-28
rfs7000-37FABE(config-device-B4-C7-99-71-17-28)#meshpoint-device no-root
rfs7000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
```

```
rfs7000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#show context
meshpoint no-root
  meshid test
  beacon-format mesh-point
  control-vlan 1
  security-mode eap
  no root
rfs7000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
```

```
rfs7000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#root
rfs7000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#show context
meshpoint no-root
  meshid test
  beacon-format mesh-point
  control-vlan 1
  security-mode eap
  root
rfs7000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the configuration of this meshpoint as a root meshpoint</td>
</tr>
</tbody>
</table>
26.1.11 **security-mode**

- **meshpoint-config-instance**

Configures the security mode for this meshpoint

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
security-mode [eap|none|psk]
```

**Parameters**

- **security-mode [eap|none|psk]**

<table>
<thead>
<tr>
<th>security-mode</th>
<th>Configures the security mode for this meshpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap</td>
<td>Uses 802.1X/EAP as the security mode. When using this option, use the <code>wpa2</code> command to specify the EAP authentication type and related parameters.</td>
</tr>
<tr>
<td>none</td>
<td>No security is configured for this meshpoint</td>
</tr>
<tr>
<td>psk</td>
<td>Uses Pre Shared Key (PSK) as the security mode. When using this option, use the <code>wpa2</code> command to enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows **root meshpoint** configuration with PSK authentication enabled:

```
rfs7000-37FABE(config-meshpoint-test)#security-mode psk
```

```
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
  description "This is an example of a meshpoint description"
  meshid TestingMeshPoint
  beacon-format mesh-point
  control-vlan 1
  allowed-vlans 1,10-16,18-23
  neighbor inactivity-timeout 300
  data-rates 2.4GHz bgn
  data-rates 5GHz an
  security-mode psk
  root
```

The following example shows **root meshpoint** configuration with EAP authentication enabled:

```
rfs7000-37FABE(config-meshpoint-root)#security-mode eap
```

```
rfs7000-37FABE(config-meshpoint-test)#
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets the security configuration for this meshpoint to “none”. This indicates that no security is configured for this meshpoint.</td>
</tr>
</tbody>
</table>
26.1.12 service

Use this command to allow only those neighbors who are capable of 802.11n data rates to associate with this meshpoint.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
service [allow-ht-only|show cli]
```

Parameters

- `service [allow-ht-only|show cli]`

<table>
<thead>
<tr>
<th>service allow-ht-only</th>
<th>Allows only those neighbors who are capable of high throughput data rates (802.11n data rates) to associate with the meshpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>service show cli</td>
<td>Displays running system configuration</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-meshpoint-test)#service allow-ht-only
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
  description "This is an example of a meshpoint description"
  meshid TestingMeshPoint
  shutdown
  beacon-format mesh-point
  control-vlan 1
  allowed-vlans 1,10-16,18-23
  neighbor inactivity-timeout 300
  data-rates 2.4GHz bgn
  data-rates 5GHz an
  security-mode psk
  wpa2 psk 0 Test Company
  wpa2 key-rotation unicast 1200
  wpa2 key-rotation broadcast 600
  root
  service allow-ht-only
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands

| no | Removes the restriction that only 802.11n capable neighbor devices can associate with this meshpoint |
| service | Invokes service commands to troubleshoot or debug |
26.1.13 shutdown

meshpoint-config-instance

Shuts down this meshpoint. Use this command to prevent an AP from participating in a mesh network.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
shutdown

Parameters
None

Examples
rfs7000-37FABE(config-meshpoint-test)#shutdown
rfs7000-37FABE(config)

Related Commands

no | Enables an AP as a meshpoint
26.1.14 use

*meshpoint-config-instance*

Uses a *Quality of Service* (QoS) policy defined specifically for meshpoints. To use this QoS policy, it must be defined. To define a meshpoint QoS policy, see *meshpoint-qos-policy-config-instance*.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

### Syntax

```plaintext
use [aaa-policy <AAA-POLICY-NAME>|meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>]
```

### Parameters

- **use [aaa-policy <AAA-POLICY-NAME>|meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `use meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>` | Configures this meshpoint to use a predefined meshpoint QoS policy
| `use aaa-policy <AAA-POLICY-NAME>` | Configures this meshpoint to use a predefined aaa-policy

### Examples

```
rfs7000-37FABE(config-meshpoint-test)#use meshpoint-qos-policy test
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
shutdown
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
neighbor inactivity-timeout 300
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode psk
root

use meshpoint-qos-policy test
rfs7000-37FABE(config-meshpoint-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the meshpoint QoS policy associated with this meshpoint</td>
</tr>
<tr>
<td><code>meshpoint-qos-policy-config-instance</code></td>
<td>Creates and configures a meshpoint QoS policy</td>
</tr>
</tbody>
</table>
### 26.1.15 wpa2

#### meshpoint-config-instance

Use this command to configure the parameters of authentication mode specified using the 'security-mode' keyword. This command also allows you to set a unicast and broadcast key rotation interval.

Supported in the following platforms:

- **Access Points** — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- **Access Points (as root APs only)** — AP650, AP622
- **Wireless Controllers** — RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

- `wpa2 [eap|psk|key-rotation]
- `wpa2 key-rotation [broadcast|unicast] <30-86400>
- `wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]
- `wpa2 eap [auth-type|identity|peap-mschapv2|tls]
- `wpa2 eap [auth-type [peap-mschapv2|tls]|identity <WORD>]
- `wpa2 eap peap-mschapv2 user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>]
  `{trustpoint <TRUSTPOINT-NAME>}
- `wpa2 eap tls trustpoint <TRUSTPOINT-NAME>

#### Parameters

- **wpa2 key-rotation [broadcast|unicast] <30-86400>**
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Enables periodic rotation of encryption keys used for broadcast and unicast traffic.</td>
</tr>
<tr>
<td>&lt;30-86400&gt;</td>
<td>Configures key rotation interval for unicast or broadcast transmission.</td>
</tr>
<tr>
<td></td>
<td>Configures key rotation interval for broadcast and multicast traffic. This option is disabled by default. When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Key rotation enhances the broadcast traffic security on the WLAN.</td>
</tr>
<tr>
<td>unicast</td>
<td>Configures key rotation interval for unicast traffic. This option is disabled by default.</td>
</tr>
</tbody>
</table>

- **wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]**
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secret [0 &lt;SECRET&gt;]</td>
<td>Configures the shared key for authentication mode PSK. If the security mode is set as ‘psk’ using the ‘security-mode’ keyword, use this command to configure the pre-shared key.</td>
</tr>
<tr>
<td>2 &lt;SECRET&gt;</td>
<td>Configures the PSK used to authenticate this meshpoint with other meshpoints in the network.</td>
</tr>
<tr>
<td>&lt;SECRET&gt;</td>
<td>Specifies the secret key. The pre-shared key can be in ASCII (8 to 63 characters in length) or Hexadecimal (not exceeding 64 characters in length) formats.</td>
</tr>
</tbody>
</table>
### wpa2 eap [auth-type [peap-mschapv2|tls]|identity <WORD>]

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wpa2 eap</strong></td>
<td>Configures the 802.1X/EAP based authentication type for this meshpoint. If the security mode is set as ‘eap’ using the ‘security-mode’ keyword, use this command to specify the EAP type. The options are: peap-mschapv2 and tls.</td>
</tr>
</tbody>
</table>

| **auth-type [peap-mschapv2|tls]** | Specifies the EAP authentication type. The options are:  
  - peap-mschapv2 – Configures EAP authentication type as Protected Extensible Authentication Protocol (PEAP) with default auth type MSCHAPv2. This is the default setting.  
  - tls – Configures EAP authentication type as Transport Layer Security (TLS)  
  *Note:* The certificate should be issued from an Enterprise or public certificate authority to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials. |

| **identity <WORD>** | Configures identity to be used during phase1 authentication  
  - <WORD> – Enter a string up to 256 characters in length (this should not be actual identity of user but some anonymous/bogus username) |

---

### wpa2 eap peap-mschapv2 user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>] {trustpoint <TRUSTPOINT-NAME>}

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wpa2 eap peap-mschapv2</strong></td>
<td>Configures PEAP-related user credentials and trustpoint details</td>
</tr>
</tbody>
</table>

| **user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>]** | Specify the user credentials used for authentication  
  - user <USER-NAME> – Specify the user name.  
  - password [0 <WORD>|2 <WORD>|<WORD>] – Specify the password associated with the specified user. |

| **trustpoint <TRUSTPOINT-NAME>** | Optional. Associates a trustpoint used for installing CA certificate and verifying server certificate  
  - <TRUSTPOINT-NAME> – Specify the trustpoint name (should be existing and configured). |

---

### wpa2 eap tls trustpoint <TRUSTPOINT-NAME>

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wpa2 eap tls</strong></td>
<td>Configures TLS client related parameters</td>
</tr>
</tbody>
</table>

| **trustpoint <TRUSTPOINT-NAME>** | Configures trustpoint details  
  - trustpoint <TRUSTPOINT-NAME> – Assigns a trustpoint to be used for installing TLS client certificate, client private key, and CA certificate  
  - <TRUSTPOINT-NAME> – Specify the trustpoint name (should be existing and configured) |
Examples

rfs7000-37FABE(config-meshpoint-test)#wpa2 key-rotation broadcast 600
rfs7000-37FABE(config-meshpoint-test)#wpa2 key-rotation unicast 1200
rfs7000-37FABE(config-meshpoint-test)#wpa2 psk Test Company

rfs7000-37FABE(config-meshpoint-test)#show context
 meshpoint test
  description "This is an example of a meshpoint description"
  meshid TestingMeshPoint
  shutdown
  beacon-format mesh-point
  control-vlan 1
  allowed-vlans 1,10-16,18-23
  neighbor inactivity-timeout 300
  data-rates 2.4GHz bgn
  data-rates 5GHz an
  security-mode psk
  wpa2 psk 0 Test Company
  wpa2 key-rotation unicast 1200
  wpa2 key-rotation broadcast 600
  root
rfs7000-37FABE(config-meshpoint-test)#

The following example shows root meshpoint configuration with EAP authentication enabled:

rfs7000-37FABE(config-meshpoint-root)#show context
 meshpoint test
  meshid test
  beacon-format mesh-point
  control-vlan 101
  allowed-vlans 101,103
  use aaa-policy test
  security-mode eap
  root
rfs7000-37FABE(config-meshpoint-test)#

The following example shows non-root meshpoint configuration with EAP PEAP-MSCHAPv2 authentication:

rfs7000-37FABE(config-meshpoint-testNoRoot)#show context
 meshpoint testNoRoot
  meshid test
  beacon-format mesh-point
  control-vlan 101
  allowed-vlans 101,103
  security-mode eap
  wpa2 eap peap-mschapv2 user tester123 password 0 testing1234 trustpoint mesh1
  wpa2 eap identity tester123
  no root
rfs7000-37FABE(config-meshpoint-testNoRoot)#

The following example shows non-root meshpoint configuration with EAP TLS authentication:

rfs7000-37FABE(config-meshpoint-testNoRoot)#show context
 meshpoint testNoRoot
  meshid test
  beacon-format mesh-point
  control-vlan 101
  allowed-vlans 101,103
  security-mode eap
  wpa2 eap peap-mschapv2 user tester123 password 0 testing1234 trustpoint mesh1
  wpa2 eap tls trustpoint mesh1
  wpa2 eap identity tester123
  no root
rfs7000-37FABE(config-meshpoint-testNoRoot)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets PSK configuration and key rotation duration</td>
</tr>
</tbody>
</table>
26.2 meshpoint-qos-policy-config-instance

Mesh QoS provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS helps ensure each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as video, voice and data. Packets within each category are processed based on the weights defined for each mesh point.

To create a meshpoint, see meshpoint-config-instance. A meshpoint QoS policy is created from the (config) instance. To create a meshpoint QoS policy use the following command:

```
<DEVICE>(config)#meshpoint-qos-policy <POLICYNAME>
```

```
rfs7000-37FABE(config)#meshpoint-qos-policy test
rfs7000-37FABE(config-meshpoint-qos-test)#
```

The following table summarizes the meshpoint-qos-policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Configures accelerated multicast parameters</td>
<td>page 26-28</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 26-30</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Configures the rate limits for this QoS policy</td>
<td>page 26-31</td>
</tr>
</tbody>
</table>
26.2.1 accelerated-multicast

meshpoint-qos-policy-config-instance

Configures the accelerated multicast stream’s address and forwarding QoS classification

NOTE: For accelerated multicast feature to work, IGMP querier must be enabled.

When a user joins a multicast stream, an entry is created in the device’s (AP or wireless controller) snoop table and the entry is set to expire after a set time period. Multicast packets are forwarded to the appropriate wireless LAN or mesh until this entry is available in the snoop table.

Snoop querier keeps the snoop table current by updating entries that are set to expire. It also keeps an entry for each multicast stream till there are users registered for the stream.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
accelerated-multicast [<MULTICAST-IP>|autodetect] {classification [background|best-effort|trust|video|voice]}

Parameters
- accelerated-multicast [<MULTICAST-IP>|autodetect] {classification [background|best-effort|trust|video|voice]}

- accelerated-multicast: Configures the accelerated multicast stream address and forwarding QoS classification

- <MULTICAST-IP>: Specify a list of multicast addresses and classifications. Packets are accelerated when the destination address matches.

- autodetect: Lets the system to automatically detect multicast streams to be accelerated

This option allows the administrator to convert multicast packets to unicast in order to provide better overall airtime utilization and performance. The system can be configured to automatically detect multicast streams and convert them to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, there are a number of classification mechanisms applied to the stream and the administrator can select what type of classification they would want. Classification types are trust, voice, video, best effort, and background.

- classification: Optional. Defines the QoS classification to apply to a multicast stream. The following options are available:
  - background
  - best effort
  - trust
  - video
  - voice
Examples

rfs7000-37FABE(config-meshpoint-qos-test)#accelerated-multicast 224.0.0.1 classification video

rfs7000-37FABE(config-meshpoint-qos-test)#show context meshpoint-qos-policy test
accelerated-multicast 224.0.0.1 classification video
rfs7000-37FABE(config-meshpoint-qos-test)#

Related Commands

| no | Resets accelerated multicast configurations for this meshpoint QoS policy |


### 26.2.2 `no`  

*meshpoint-qos-policy-config-instance*

Negates the commands for meshpoint QoS policy or resets their values to their default

**Supported in the following platforms:**

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [accelerated-multicast|rate-limit]
no accelerated-multicast [<MULTICAST-IP>|autodetect]
no rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size|rate}
no rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background|best-effort|video|voice]}
```

**Parameters**

- `no <PARAMETERS>`

  | `no <PARAMETERS>` | Removes or reverts this meshpoint QoS policy settings to default based on the parameters passed |

**Examples**

```bash
rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
  rate-limit meshpoint from-air rate 80000
  rate-limit meshpoint from-air red-threshold video 80
  rate-limit meshpoint from-air red-threshold voice 70
  accelerated-multicast 224.0.0.1 classification video

rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air rate
rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-threshold video 80
rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-threshold voice 70
rfs7000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
  accelerated-multicast 224.0.0.1 classification video
```

rfs7000-37FABE(config-meshpoint-qos-test)#
26.2.3 rate-limit

meshpoint-qos-policy-config-instance

Configures the rate limiting of traffic on a per meshpoint or per neighbor basis.

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic, bombardments and interference are caused by numerous sources, such as network loops, faulty devices, or malicious software (such as a worm or virus) that has infected one or more branch-level devices. Rate limiting limits the maximum rate sent to or received from the wireless network (and meshpoint) per neighbor. It prevents any single user from overwhelming the wireless network. It also provides differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the network and data transmitted from a mesh point's neighbor.

Before defining rate limit thresholds for meshpoint transmit and receive traffic, it is recommended that you define the normal number of ARP, broadcast, multicast, and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

Supported in the following platforms:
• Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
• Access Points (as root APs only) — AP650, AP622
• Wireless Controllers — RFS6000, RFS7000
• Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9510, NX9520, NX9600

Syntax
rate-limit [meshpoint|neighbor]
rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>|
rate <50-1000000>]
rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background <0-100>|
best-effort <0-100>|video <0-100>|voice <0-100>]}|

Parameters
• rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>|
rate <50-1000000>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint</td>
<td>Configures rate limit parameters for all data received from any meshpoint in the mesh network. This option is disabled by default.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Configures rate limit parameters for neighboring meshpoint devices. Enables rate limiting for data transmitted from the client to its associated access point radio and connected controller. This option is disabled by default.</td>
</tr>
<tr>
<td>from-air</td>
<td>Configures rate limits for traffic from the wireless neighbor to the network.</td>
</tr>
<tr>
<td>to-air</td>
<td>Configures rate limits for traffic from the network to the wireless neighbor.</td>
</tr>
<tr>
<td>max-burst-size</td>
<td>Optional. Configures the maximum burst size in kilobytes. Set a value from 2 - 1024 kbytes.</td>
</tr>
<tr>
<td>&lt;2-1024&gt;</td>
<td>For a meshpoint: The smaller the burst, the less likely that the transmit packet transmission results in congestion for the meshpoint's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320 kbytes. Contd..</td>
</tr>
</tbody>
</table>
For a neighbor: The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

<table>
<thead>
<tr>
<th>rate &lt;50-1000000&gt;</th>
<th>Optional. Defines a receive or transmit rate limit in kilobytes per second. Set a value from 50 - 1000000 kbps. For a meshpoint: This limit constitutes a threshold for the maximum the number of packets transmitted or received over the meshpoint (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps. For a neighbor: This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint</td>
<td>Configures rate limit parameters for a meshpoint</td>
</tr>
<tr>
<td>neighbor</td>
<td>Configures rate limit parameters for neighboring meshpoint devices</td>
</tr>
<tr>
<td>from-air</td>
<td>Configures rate limits for traffic from the wireless neighbor to the network</td>
</tr>
<tr>
<td>to-air</td>
<td>Configures rate limit value for traffic from the network to the wireless neighbor</td>
</tr>
<tr>
<td>red-threshold</td>
<td>Optional. Configures random early detection threshold (RED threshold) for traffic class</td>
</tr>
<tr>
<td>background &lt;0-100&gt;</td>
<td>The following keyword is applicable to the ‘from-air’ and ‘to-air’ traffics. Configures the threshold for low priority (background) traffic For a meshpoint: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. For a neighbor: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.</td>
</tr>
<tr>
<td>best-effort &lt;0-100&gt;</td>
<td>The following keyword is applicable to the ‘from-air’ and ‘to-air’ traffics. Configures the threshold for best effort traffic For a meshpoint: This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. For a neighbor: This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.</td>
</tr>
<tr>
<td><strong>video &lt;0-100&gt;</strong></td>
<td>The following keyword is applicable to the ‘from-air’ and ‘to-air’ traffics. Configures the threshold for video traffic. For a meshpoint: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. For a neighbor: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.</td>
</tr>
<tr>
<td><strong>voice &lt;0-100&gt;</strong></td>
<td>The following keyword is applicable to the ‘from-air’ and ‘to-air’ traffics. Configures the threshold for voice traffic. For a meshpoint: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. For a neighbor: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0% and implies no early random drops will occur.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air max-burst-size 800
rfs7000-37FABE(config-meshpoint-qos-test)#show context meshpoint-qos-policy test rate-limit meshpoint from-air max-burst-size 800 accelerated-multicast 224.0.0.1 classification video
rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air rate 80000
rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-threshold video 80
rfs7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-threshold voice 70
rfs7000-37FABE(config-meshpoint-qos-test)#show context meshpoint-qos-policy test rate-limit meshpoint from-air rate 80000 rate-limit meshpoint from-air max-burst-size 800 rate-limit meshpoint from-air red-threshold video 80 rate-limit meshpoint from-air red-threshold voice 70 accelerated-multicast 224.0.0.1 classification video
```

**Related Commands**

| **no** | Resets traffic rate limit settings for this meshpoint QoS policy |
26.3 meshpoint-device-config-instance

The following table lists the meshpoint device configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint-device</td>
<td>Configures an access point as a meshpoint device and enters its configuration mode</td>
<td>page 26-35</td>
</tr>
<tr>
<td>meshpoint-device-commands</td>
<td>Invokes the meshpoint-device configuration commands</td>
<td>page 26-37</td>
</tr>
</tbody>
</table>
26.3.1 *meshpoint-device*

This command configures an access point to use a defined meshpoint. This command is available only under the AP622, AP650, AP6522, AP6532, AP71XX, AP81XX, AP82XX device or profile context. To configure this feature use one of the following options:

- navigate to the device profile config context (used when configuring access point profile on a controller)
- navigate to the device’s config context using the self command (used when configuring a logged on access point)

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

**Syntax**

```
meshpoint-device <MESHPOINT-NAME>
```

**Parameters**

- `meshpoint-device <MESHPOINT-NAME>`

<table>
<thead>
<tr>
<th><code>meshpoint-device</code></th>
<th>Configures the AP as a meshpoint device and sets its parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MESHPOINT-NAME&gt;</code></td>
<td>The meshpoint to configure the AP with (should be existing and configured)</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#profile ap71xx AP71XXTestProfile
rfs7000-37FABE(config-profile-AP71XXTestProfile)#meshpoint-device test
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Mesh Point Device Mode commands:

```
acs          Configure auto channel selection parameters
exclude      Exclude neighboring Mesh Devices
hysteresis   Configure path selection SNR hysteresis values
monitor      Event Monitoring
no           Negate a command or set its defaults
path-method  Path selection method used to find a root node
preferred    Configure preferred path parameters
root         Set this meshpoint as root
root-select  Root selection method parameters
clrscr       Clears the display screen
commit       Commit all changes made in this session
do           Run commands from Exec mode
end          End current mode and change to EXEC mode
exit         End current mode and down to previous mode
help         Description of the interactive help system
revert       Revert changes
service      Service Commands
show         Show running system information
write        Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#meshpoint-device test
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#?

Mesh Point Device Mode commands:

- **acs** Configure auto channel selection parameters
- **exclude** Exclude neighboring Mesh Devices
- **hysteresis** Configure path selection SNR hysteresis values
- **monitor** Event Monitoring
- **no** Negate a command or set its defaults
- **path-method** Path selection method used to find a root node
- **preferred** Configure preferred path parameters
- **root** Set this meshpoint as root
- **root-select** Root selection method parameters
- **clrscr** Clears the display screen
- **commit** Commit all changes made in this session
- **do** Run commands from Exec mode
- **end** End current mode and change to EXEC mode
- **exit** End current mode and down to previous mode
- **help** Description of the interactive help system
- **revert** Revert changes
- **service** Service Commands
- **show** Show running system information
- **write** Write running configuration to memory or terminal

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#?
### 26.3.2 meshpoint-device-commands

*meshpoint-device-config-instance*

The following table lists the meshpoint-device configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>acs</td>
<td>Enables <em>Automatic Channel Selection</em> (ACS) on this meshpoint device (access point)</td>
<td>page 26-38</td>
</tr>
<tr>
<td>exclude</td>
<td>Excludes neighboring mesh devices</td>
<td>page 26-43</td>
</tr>
<tr>
<td>hysteresis</td>
<td>Configures path selection SNR hysteresis values on this meshpoint-device (access point)</td>
<td>page 26-44</td>
</tr>
<tr>
<td>monitor</td>
<td>Enables monitoring of critical resource and primary port links on a meshpoint device</td>
<td>page 26-45</td>
</tr>
<tr>
<td>path-method</td>
<td>Configures the method used to select the path to the root node in a mesh network</td>
<td>page 26-46</td>
</tr>
<tr>
<td>preferred</td>
<td>Configures the preferred path parameters for a meshpoint device</td>
<td>page 26-47</td>
</tr>
<tr>
<td>root</td>
<td>Configures a meshpoint device as the root meshpoint</td>
<td>page 26-48</td>
</tr>
<tr>
<td>root-select</td>
<td>Configures this meshpoint device as the cost root</td>
<td>page 26-50</td>
</tr>
<tr>
<td>no</td>
<td>Negates the commands for a meshpoint device or resets values to default</td>
<td>page 26-51</td>
</tr>
</tbody>
</table>
26.3.2.1 acs

Enables Automatic Channel Selection (ACS) on this meshpoint device (access point). When enabled, this feature automatically selects the best channel for a meshpoint-device radio based on the device configuration, channel conditions, and network layout.

In a wireless network deployment, it is advantageous for network devices to have the ability to operate in multiple channels and not be limited to only a single channel. Multiple channels increase the bandwidth and throughput of the wireless network. In such a scenario, each network device must have a mechanism to dynamically select a suitable channel of operation. ACS provides the required mechanism for a MCX enabled device.

Use this command to configure the ACS settings and override the default meshpoint configurations.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax
acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|ocs-frequency|path-min|path-threshold|preferred-interface-tolerance-period|preferred-radio-interface|priority-meshpoint|sample-count|snr-delta|signal-threshold|tolerance-period]
acs channel-hold-time [2.4GHz|5GHz] <0-86400>
acs channel-switch-delta [2.4GHz|5GHz] <5-35>
acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|80MHz|auto]
acs ocs-duration [2.4GHz|5GHz] <20-250>
acs ocs-frequency [2.4GHz|5GHz] <1-60>
acs path-min [2.4GHz|5GHz] <100-20000>
acs path-threshold [2.4GHz|5GHz] <800-65535>
acs preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>
acs preferred-radio-interface [2.4GHz|5GHz] <0-2>
acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>
acs sample-count [2.4GHz|5GHz] <1-10>
acs snr-delta [2.4GHz|5GHz] <1-100>
acs signal-threshold [2.4GHz|5GHz] <-100-0>
acs tolerance-period [2.4GHz|5GHz] <10-600>

Parameters
- acs channel-hold-time [2.4GHz|5GHz] <0-86400>

<p>| acs                  | Configures ACS settings and overrides on the selected meshpoint-device |</p>
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
</table>
| **channel-hold-time**<br>[2.4GHz|5GHz] <0-86400> | Configures the minimum time, in seconds, before a periodic scan, to assess channel conditions for a meshpoint root, is triggered.  
- 2.4GHz – Configures the channel hold interval for the 2.4GHz radio band  
- 5.0GHz – Configures the channel hold interval for the 5.0GHz radio band  
The following keyword is common to the ‘2.4GHz’ and ‘5.0GHz’ bands:  
- <0-86400> – Specify a value from 0 - 86400 seconds. The default is 1800 seconds.  
**Note:** A value of ‘0’ disables periodic channel assessment. |
| **acs channel-switch-delta**<br>[2.4GHz|5GHz] <5-35> | Configures the difference in interference between the current and best channel needed to trigger a channel change. Once the difference in the current channel and the best channel interference equals the configured value, a channel change is triggered.  
- 2.4GHz – Configures the channel switch delta for the 2.4GHz radio band  
- 5.0GHz – Configures the channel switch delta for the 5.0GHz radio band  
The following keyword is common to the ‘2.4GHz’ and ‘5.0GHz’ bands:  
- <5-35> – Specify a value from 5 - 35 dBm. The default is 10 dBm. |
| **acs channel-width**<br>[2.4GHz|5GHz]<br>[20MHz|40MHz|80MHz|auto] | Configures the channel width that meshpoint auto channel selection assigns to the radio  
- 2.4 GHz – Configures the operating channel width for the 2.4 GHz radio band  
- 5.0 GHz – Configures the operating channel width for the 5.0 GHz radio band  
The following keywords are common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- 20 MHz – Assigns the 20 MHz channel width to the radio  
- 40 MHz – Assigns the 40 MHz channel width to the radio  
- 80 MHz – Assigns the 80 MHz channel width to the radio  
- auto – Selects and assigns the best possible channel from the 20/40/80 MHz width. This is the default setting. |
| **acs ocs-duration**<br>[2.4GHz|5GHz] <20-250> | Configures the duration, in milliseconds, of off-channel scans (OCSs)  
- 2.4 GHz – Configures the ocs-duration for the 2.4 GHz radio band  
- 5.0 GHz – Configures the ocs-duration for the 5.0 GHz radio band  
The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- <20-250> – Specify a value from 20 - 250 milliseconds. The default value is 50 milliseconds. |
<p>| <strong>acs ocs-frequency</strong>&lt;br&gt;[2.4GHz|5GHz] &lt;1-60&gt; | Configures ACS settings and overrides on the selected meshpoint-device |</p>
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
</table>
| `ocs-frequency` | Configures the interval, in seconds, at which off-channel scan is performed. An ocs-frequency of 10 seconds means that an off-channel scan will be performed once every 10 seconds.  
- 2.4 GHz – Configures the ocs-frequency for the 2.4 GHz radio band  
- 5.0 GHz – Configures the ocs-frequency for the 5.0 GHz radio band  
The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- `<1-60>` – Specify a value form 1 - 60 seconds. The default is 6 seconds. |
| `acs path-min [2.4GHz|5GHz] <100-20000>` | Configures the minimum root path metric needed for auto channel selection. This is the acceptance root path metric value to consider a root as a possible candidate mesh node.  
- 2.4 GHz – Configures the minimum root path metric for the 2.4 GHz radio band  
- 5.0 GHz – Configures the minimum root path metric for the 5.0 GHz radio band  
The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- `<900-65535>` – Specify a value from 100 - 20000. The default is 1000. |
| `acs path-threshold [2.4GHz|5GHz] <800-65535>` | Configures the root path metric threshold for auto channel selection. This is the acceptance root path metric threshold beyond which the root bound to is considered as bad.  
- 2.4 GHz – Configures the root path metric threshold for the 2.4 GHz radio band  
- 5.0 GHz – Configures the root path metric threshold for the 5.0 GHz radio band  
The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- `<800-65535>` – Specify a value from 800 - 65535. The default is 1500. |
| `acs preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>` | Configures the maximum tolerance period, in seconds, for low root metrics on the preferred interface. This is the duration to wait before triggering an automatic channel selection for the next mesh-hop on the preferred interface.  
- 2.4 GHz – Configures the maximum tolerance period for the 2.4 GHz radio band  
- 5.0 GHz – Configures the maximum tolerance period for the 5.0 GHz radio band  
The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- `<800-65535>` – Specify a value from 10 - 600 seconds. |
| `acs preferred-radio-interface [2.4GHz|5GHz] <0-2>` | Configures the preferred radio interface on dual band APs  
- 2.4 GHz – Configures the preferred radio interface for the 2.4 GHz radio band  
- 5.0 GHz – Configures the preferred radio interface for the 5.0 GHz radio band  
The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:  
- `<0-2>` – Specify a value from 0 - 2. A value of 0 (zero) indicates no preferred radio. |
### ACS Settings

#### Priority Meshpoint

- **priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>**
  
  Configures the priority meshpoint. Configuring a priority meshpoint overrides automatic meshpoint configuration.
  
  - **2.4 GHz** – Configures the priority meshpoint for the 2.4 GHz radio band
  - **5.0 GHz** – Configures the priority meshpoint for the 5.0 GHz radio band

  The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:
  - `<MESHPOINT-NAME>` – Specify the meshpoint name for the selected radio band.

#### Sample Count

- **sample-count [2.4GHz|5GHz] <1-10>**
  
  Configures the minimum number of scan cycle samples to consider for auto channel selection.
  
  - **2.4 GHz** – Configures the sample count for the 2.4 GHz radio band
  - **5.0 GHz** – Configures the sample count for the 5.0 GHz radio band

  The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:
  - `<1-10>` – Specify a value from 1 -10. The default is 5 samples.

#### SNR Delta

- **snr-delta [2.4GHz|5GHz] <1-100>**
  
  Configures the channel SNR delta. A meshpoint on a candidate channel must have a SNR of a greater delta than the next hop on the current channel.
  
  - **2.4 GHz** – Configures the snr-delta for the 2.4 GHz radio band
  - **5.0 GHz** – Configures the snr-delta for the 5.0 GHz radio band

  The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:
  - `<1-100>` – Specify a value from 1 - 100 dB. The default is 5 dB.

#### Signal Threshold

- **signal-threshold [2.4GHz|5GHz] <-100-0>**
  
  Configures the signal strength threshold. If the signal strength of the next hop drops below the configured signal-threshold, a scan is triggered.
  
  - **2.4 GHz** – Configures the signal-threshold for the 2.4 GHz radio band
  - **5.0 GHz** – Configures the signal-threshold for the 5.0 GHz radio band

  The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:
  - `<-100-0>` – Specify a value from -100 - 0 dB. The default is -65 dB.

#### Tolerance Period

- **tolerance-period [2.4GHz|5GHz] <10-600>**
  
  Configures the maximum tolerance period in seconds. This is the interval to wait for the root bound to recovery from a bad link.
  
  - **2.4 GHz** – Configures the tolerance-period for the 2.4 GHz radio band
  - **5.0 GHz** – Configures the tolerance-period for the 5.0 GHz radio band

  The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands:
  - `<10-600>` – Specify a value from 10 - 600 seconds. The default is 60 seconds.
**Examples**

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs channel-hold-time 2.4GHz 2500

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-duration 2.4GHz 30

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-frequency 2.4GHz 1

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context meshpoint-device test

    acs ocs-frequency 2.4GHz 1
    acs ocs-duration 2.4GHz 30
    acs channel-hold-time 2.4GHz 2500

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reverts the configured ACS settings to default</td>
</tr>
</tbody>
</table>
26.3.2.2 exclude

> meshpoint-device-commands

Enables wired-peer (that are wired MiNT level-1 neighbors) exclusion

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax
exclude wired-peer mint-level-1

Parameters
- exclude wired-peer mint-level-1

<table>
<thead>
<tr>
<th>exclude wired-peer</th>
<th>Excludes neighboring mesh devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>wired-peer mint-level-1</td>
<td>Excludes neighboring wired mesh devices with MiNTlevel-1 link</td>
</tr>
<tr>
<td></td>
<td>When enabled, all neighboring wired mesh devices are excluded from mesh links.</td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#exclude wired-peer mint-level-1

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
meshpoint-device test
exclude wired-peer mint-level-1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#

Related Commands
- no | Disables wired-peer exclusion on this meshpoint
26.3.2.3 hysteresis

meshpoint-device-commands

Configures path selection SNR hysteresis values on this meshpoint-device (access point). These are settings that facilitate dynamic path selection. Configuring hysteresis prevents frequent re-ranking of the shortest path cost.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax

```
hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]
hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-100>|snr-delta <1-100>]
```

Parameters

- **min-threshold** `-100-0> Configures the minimum signal strength that a device should have to be considered a likely candidate in the mesh route (to the mesh root node) selection process.
  - `-100-0>` – Specify a value from -100 - 0 dB. The default is 0 dB.

- **period** `<0-600>` Configures the interval, in seconds, for which a likely candidate’s path method hysteresis is sustained. In other words a device capable of sustaining the signal strength for the specified period of time is a likely candidate in the mesh route (to the mesh root node) selection process.
  - `<0-600>` – Specify a value from 0 - 600 seconds. The default is 1 second.

- **root-sel-snr-delta** `<1-100>` Configures the signal strength, in dB, that a device has to sustain, within the delta range, to be considered a likely candidate in the mesh route (to the mesh root node) selection process.
  - `<1-100>` – Specify a value from 1 - 100 dB.

- **snr-delta** `<1-100>` Configures the SNR delta. The device with must have a SNR of a greater delta than its current neighbor to be considered a likely candidate in the mesh route (to the mesh root) selection process.
  - `<1-100>` – Specify a value from 1 - 100 dB. The default is 1 dB.

Examples

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis period 15
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis root-sel-snr-delta 12
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis snr-delta 3
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis min-threshold -65

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
meshpoint-device test
  hysteresis period 15
  hysteresis snr-delta 3
  hysteresis root-sel-snr-delta 12
  hysteresis min-threshold -65
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands

- `no` Removes the configured path selection SNR hysteresis values
26.3.2.4 **monitor**

*meshpoint-device-commands*

Enables monitoring of critical resource and primary port links. It also configures the action taken in case a critical resource goes down or a primary port link is lost.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

**Syntax**

```plaintext
monitor [critical-resource|primary-port-link-loss] action no-root
```

**Parameters**
- `monitor [critical-resource|primary-port-link-loss] action no-root`

<table>
<thead>
<tr>
<th>critical-resource</th>
<th>Enables critical resource down event monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary-port-link-loss</td>
<td>Enables primary port link loss event monitoring</td>
</tr>
<tr>
<td>action no-root</td>
<td>The following are common to all of the above:</td>
</tr>
<tr>
<td></td>
<td>• action – Sets the action taken if a critical resource goes down or if a primary port link is lost</td>
</tr>
<tr>
<td></td>
<td>• no-root – Changes the meshpoint to be non root (this is the action taken in case any of the above mentioned two events occur)</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context meshpoint-device test name test
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

**Related Commands**

| `no` | Disables monitoring of critical resource and primary port links. |
26.3.2.5 path-method

meshpoint-device-commands

Configures the path selection method used on a meshpoint device. This is the method used to select the route to the root node within a mesh network.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax

path-method [bound-pair|mobile-snr-leaf|snr-leaf|uniform]

Parameters

- path-method [bound-pair|mobile-snr-leaf|snr-leaf|uniform]

<table>
<thead>
<tr>
<th>path-method</th>
<th>Sets the method used to select the path to the root node in a mesh network</th>
</tr>
</thead>
<tbody>
<tr>
<td>bound-pair</td>
<td>Enables a meshpoint to form an exclusive path with only one other meshpoint. Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied.</td>
</tr>
<tr>
<td>mobile-snr-leaf</td>
<td>Configures the path selection method as mobile-snr-leaf. When selected, the path to the root node is selected based on the Signal-to-Noise Ratio (SNR) to a neighboring device. This option allows meshpoint devices to select a neighbor with the strongest SNR. Meshpoint devices using the mobile-snr-leaf method are non-forwarding nodes in the meshpoint traffic. Note: Select this option for Vehicular Mounted Modem (VMM) access points or other mobile devices.</td>
</tr>
<tr>
<td>snr-leaf</td>
<td>This option allows meshpoints to select a neighbor with the strongest SNR. It is similar to the mobile-snr-leaf option, but is not applicable to mobile devices, such as VMMs.</td>
</tr>
<tr>
<td>uniform</td>
<td>Indicates the path selection method is uniform. When selected, two paths will be considered equivalent if the average goodput is the same for both paths. This is the default setting. Note: Select this option for infrastructure devices.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#path-method mobile-snr-leaf

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context meshpoint-device TEST
  name TEST
  path-method mobile-snr-leaf
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

Related Commands

no                   | Resets the path selection method on a meshpoint device |
26.3.2.6 preferred

**meshpoint-device-commands**

Configures the preferred path parameters for this meshpoint device

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

**Syntax**

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]
```

**Parameters**

- `preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]`

<table>
<thead>
<tr>
<th>preferred</th>
<th>Configures the preferred path parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor &lt;MAC&gt;</td>
<td>Adds the MAC address of a neighbor meshpoint as a preferred neighbor</td>
</tr>
<tr>
<td>root &lt;MAC&gt;</td>
<td>Adds the MAC address of a root meshpoint as a preferred root</td>
</tr>
<tr>
<td>interface [2.4GHz</td>
<td>4.9GHz</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred neighbor 11-22-33-44-55-66
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred root 22-33-44-55-66-77
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred interface 5GHz
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context meshpoint-device test
  name test
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

**Related Commands**

| no | Removes the configuration of preferred paths for this meshpoint device |
26.3.2.7 root

Configure this meshpoint device as the root meshpoint

You can optionally use the select-method option to enable dynamic mesh selection. When enabled, this option overrides root or no-root configuration and uses the selection method.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax

```
root {select-method [auto-mint|auto-proximity]}
```

Parameters

- `root {select-method [auto-mint|auto-proximity]}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>select-method</td>
<td>Optional. Enables dynamic mesh selection. When enabled, this option overrides root or no-root configuration and chooses the selection method.</td>
</tr>
<tr>
<td>auto-mint</td>
<td>- Enables dynamic root selection using Auto-MiNT (based on path cost)</td>
</tr>
<tr>
<td>auto-proximity</td>
<td>- Enables dynamic root selection using meshpoint proximity. When auto-proximity is selected, root selection is based on signal strength of candidate roots.</td>
</tr>
</tbody>
</table>

Note: The Auto-MiNT or Cost Method dynamically determines the root/non-root configuration of a meshpoint by:

- Monitoring and ranking the signal strength and path cost of neighboring mesh points.
- Setting the configuration to:
  - non-root: If the link with the shortest path to the cost-root mesh device is a MCX meshpoint link
  - root: If the link with the shortest path to the cost-root mesh device is a non MCX meshpoint link (wired link).
- This requires that the meshpoint device, in the brain car, be configured as the ‘cost root’ and the ‘cost root’ meshpoint-device be the l2 gateway to the controller. Use the `root-select > cost-root` command to configure a meshpoint-device as ‘cost-root’.
  - Using signal strength of neighboring meshpoint as the sole metric to determine the next mesh hop to the root.
  - Loop detection with both meshpoints in a car select non-root and form a mesh link with the same root.

Examples

```
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
meshpoint-device test
  name test
  root
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root select-method auto-mint

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context meshpoint-device test
  root select-method auto-mint
  
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the configuration of this meshpoint device as a root meshpoint. Also allows you to disable dynamic mesh selection (if enabled).</td>
</tr>
</tbody>
</table>
26.3.2.8 root-select

meshpoint-device-commands

Configures this meshpoint device as the cost root

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax
oot-select cost-root

Parameters

- root-select cost-root

Examples

ap7131-11B6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root-select cost-root

ap7131-11B6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context

root select-method auto-mint

root-select cost-root

ap7131-11B6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#

Related Commands

- no

  Removes this meshpoint-device as the cost-root
26.3.2.9 no

meshpoint-device-commands

Negates the commands for a meshpoint device or resets values to default.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7532, AP7562, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax

no [acs|exclude|hysteresis|monitor|path-method|preferred|root|root-select]

no acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|
ocs-frequency|path-min|path-threshold|preferred-interface-tolerance-period|
preferred-radio-interface|priority-meshpoint|sample-count|snr-delta|
signal-threshold|tolerance-period] [2.4GHZ|5GHz]

no exclude wired-peer mint-level-1

no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]

no monitor [critical-resource|primary-port-link-loss]

no [path-method|root {select-method}]

no root-select cost-root

no preferred [interface|root|neighbor]

Parameters
- no <PARAMETERS>

no <PARAMETERS> Removes or reverts this meshpoint device settings to default based on the parameters passed.

Examples

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
meshpoint-device test
  name test
    root
      preferred root 22-33-44-55-66-77
      preferred neighbor 11-22-33-44-55-66
      preferred interface 5GHz
    monitor critical-resource action no-root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no monitor
critical-resource
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no preferred neighbor
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no root
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no preferred interface
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
meshpoint-device test
  name test
  no root
    preferred root 22-33-44-55-66-77
rfs7000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
There has been an exponential increase in the number and types of Wi-Fi mobile devices being used globally, resulting in a phenomenal growth in the data traffic volume. Consequently, the demand for secure, quick, and unlicensed access to public Wi-Fi hotspots, capable of handling this sudden influx of mobile data traffic, has been increasing. However, public hotspots have certain intrinsic usability issues, such as network discovery and selection, traffic prioritization, roaming capabilities, user authentication etc. The IEEE 802.11u standards (includes Hotspot 2.0 protocol extensions) were introduced to address these issues.

Hotspot 2.0 is a Wi-Fi Alliance standard that enables interoperability between clients, infrastructure, and operators. It makes a portion of the IEEE 802.11u standard mandatory and adds Hotspot 2.0 extensions that allow clients to query a network before actually attempting to join it. For example, you are using a laptop at an airport and have a list of SSIDs to select from. You will have to first identify the SSID you have the credentials for and then connect to the network. This can be time consuming. In such a scenario, a Hotspot 2.0 enabled device would present only those SSIDs for which you possess credentials. In short Hotspot 2.0 allows devices to query a network for configuration details, such as WAN metrics, network type, hotspot service provider details, and domain names without actually connecting to the network.

Hotspot 2.0 enabled clients can identify a Hotspot 2.0 capable access point (AP) from the new elements present in the APs beacon/probe messages. Having ascertained that an AP is Hotspot 2.0 capable, the client uses action frames to send an Access Network Query Protocol (ANQP) query inside a Generic Advertisement Service (GAS) request. The AP responds with an action frame containing an ANQP response within a GAS response. Based on this response the mobile device determines the type of credentials needed to log on to the AP.

The WING Wi-Fi Alliance implementation defines a passpoint policy that allows a single or a set of Hotspot 2.0 configuration to be global and referenced by the devices that use it. This policy is applied to APs to make them Hotspot 2.0 Wi-Fi Alliance compliant. The passpoint policy is mapped to a WLAN. However, only primary WLANs on a BSSID will have their passpoint policy configuration used. For more information, see Chapter 4, GLOBAL CONFIGURATION COMMANDS.
To migrate to the passpoint policy configuration mode, use the following command:

```
<DEVICE>(config)#passpoint-policy <POLICY-NAME>
```

```
rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#
```

```
rfs4000-229D58(config-passpoint-policy-test).offsetTop?
```

Passpoint Policy Mode commands:

- 3gpp: Configure a 3gpp plmn (public land mobile network) id
- access-network-type: Set the access network type for the hotspot
- connection-capability: Configure the connection capability for the hotspot
- domain-name: Add a domain-name for the hotspot
- hessid: Set a homogeneous ESSID value for the hotspot
- internet: Advertise the hotspot having internet access
- ip-address-type: Configure the advertised ip-address-type
- nai-realm: Configure a NAI realm for the hotspot
- net-auth-type: Add a network authentication type to the hotspot
- no: Negate a command or set its defaults
- operator: Add configuration related to the operator of the hotspot
- osu: Online signup
- roam-consortium: Add a roam consortium for the hotspot
- venue: Set the venue parameters of the hotspot
- wan-metrics: Set the wan-metrics of the hotspot
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- service: Service Commands
- show: Show running system information
- write: Write running configuration to memory or terminal

```
rfs4000-229D58(config-passpoint-policy-test).offsetTop
```

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
## 27.1 passpoint-policy

The following table summarizes passpoint policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>Configures a 3rd Generation Partnership Project (3gpp) Public Land Mobile Network (PLMN) ID</td>
<td>page 27-4</td>
</tr>
<tr>
<td>access-network-type</td>
<td>Configures the access network type element in this hotspot</td>
<td>page 27-5</td>
</tr>
<tr>
<td>connection-capability</td>
<td>Configures the connection capability element in this passpoint policy</td>
<td>page 27-6</td>
</tr>
<tr>
<td>domain-name</td>
<td>Configures the RF Domains to which this hotspot is applicable</td>
<td>page 27-8</td>
</tr>
<tr>
<td>hessid</td>
<td>Configures the Homogeneous Extended Service Set Identifier (HESSID) for a specified hotspot zone</td>
<td>page 27-9</td>
</tr>
<tr>
<td>internet</td>
<td>Advertises the availability of Internet access in this hotspot</td>
<td>page 27-10</td>
</tr>
<tr>
<td>ip-address-type</td>
<td>Advertises the IP address type used in this hotspot.</td>
<td>page 27-11</td>
</tr>
<tr>
<td>nai-realm</td>
<td>Configures a Network Access Identifier (NAI) realm name and enters its configuration mode</td>
<td>page 27-13</td>
</tr>
<tr>
<td>net-auth-type</td>
<td>Configures the network authentication type used in this hotspot</td>
<td>page 27-18</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts passpoint policy configuration</td>
<td>page 27-19</td>
</tr>
<tr>
<td>operator</td>
<td>Configures the operator friendly name for this hotspot</td>
<td>page 27-20</td>
</tr>
<tr>
<td>osu</td>
<td>Configures an online sign up (OSU) SSID/provider and enters its configuration mode</td>
<td>page 27-21</td>
</tr>
<tr>
<td>roam-consortium</td>
<td>Configures the list of Roaming Consortium Organization Identifiers (OIs) supported on this hotspot</td>
<td>page 27-31</td>
</tr>
<tr>
<td>venue</td>
<td>Configures the venue group and type for this passpoint policy</td>
<td>page 27-32</td>
</tr>
<tr>
<td>wan-metrics</td>
<td>Configures the WAN performance metrics for this hotspot</td>
<td>page 27-36</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
27.1.1 3gpp

passpoint-policy

Configures a 3rd Generation Partnership Project (3GPP) Public Land Mobile Network (PLMN) information. The 3GPP PLMN information is a combination of the Mobile Country Code (MCC) and Mobile Network Code (MNC). This MCC and MNC combination uniquely identifies a cellular operator. For example, Telstar Corporation Ltd. in Australia is identified by MCC 505 and MNC 001.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX7562, NX9000, NX9600

Syntax

3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}

Parameters

- 3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}

| 3gpp | Configures the 3GPP PLMN information that is returned in response to an ANQP query |
| mcc <MOBILE-COUNTRY-CODE> | Specifies the MCC. The MCC is a two or three digit decimal value. For example, the MCC for Australia is 505. |
| mnc <MOBILE-NETWORK-CODE> | Specifies the MNC. The MNC is a two or three decimal value used in combination with the MCC to uniquely identify a mobile network operator. The MNC and MCC combination (also known as the MCC/MNC tuple) forms the first five or six digits of the International Mobile Subscriber's Identity (IMSI). **Note:** If the MCC and MNC values are not configured, the hotspot will not return the element in an ANQP capability request and ignores any ANQP query for the element. |
| description <LINE> | Optional. Configures a description that uniquely identifies this PLMN. Provide a description not exceeding 64 characters in length. |

Examples

```
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
  3gpp mcc 310 mnc 970
  3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

```
no
```

Removes the specified 3gpp PLMN information and its corresponding MCC/MNC settings
27.2 access-network-type

Configures the access network type for this hotspot. The beacons and probe responses communicate the type of hotspot (public, private, guest-use, emergency etc.) to clients seeking access.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax
access-network-type [chargeable-public|emergency-services|experimental|free-public|personal-device|private|private-guest|wildcard]

Parameters
- access-network-type [chargeable-public|emergency-services|experimental|free-public|personal-device|private|private-guest|wildcard]

<table>
<thead>
<tr>
<th>access-network-type</th>
<th>Select the access network type for this hotspot. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• chargeable-public – The network type is a chargeable public network</td>
</tr>
<tr>
<td></td>
<td>• emergency-services – The network is used to provide emergency services only</td>
</tr>
<tr>
<td></td>
<td>• experimental – The network is used for test or experimental purposes only</td>
</tr>
<tr>
<td></td>
<td>• free-public – The network type is a free public</td>
</tr>
<tr>
<td></td>
<td>• personal-device – The network is used for personal devices only</td>
</tr>
<tr>
<td></td>
<td>• private – The network is a private network</td>
</tr>
<tr>
<td></td>
<td>• private-guest – The network is a private network with guest access (default setting)</td>
</tr>
<tr>
<td></td>
<td>• wildcard – Includes all access network types</td>
</tr>
</tbody>
</table>

Note: If the network type is set to chargeable-public, probe responses advertise this hotspot as a chargeable-public hotspot.

Examples
rfs4000-229D58(config-passpoint-policy-test)#access-network-type chargeable-public
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy_test
access-network-type chargeable-public
3gpp mcc 310 mnc 970
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

| no | Reverts to the default access network type setting (private) |
27.1.3 connection-capability

passpoint-policy

Configures the connection capability element in this passpoint policy. When configured, it communicates which ports are open or closed on the Hotspot, in response to an ANQP query.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax

connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]

connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]
[closed|open|unknown]

connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]

Parameters

- connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn] [closed|open|unknown]
- connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]

<table>
<thead>
<tr>
<th>connection-capability</th>
<th>Configures the connection capability element in this passpoint policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>Specifies the protocol type as FTP. Configures TCP port 20.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the protocol type as HTTP. Configures TCP port 80.</td>
</tr>
<tr>
<td>icmp</td>
<td>Specifies the protocol type as ICMP.</td>
</tr>
<tr>
<td>ipsec-vpn</td>
<td>Specifies the protocol type as IPSEC VPN. Configures ESP and UDP ports 500 and 4500.</td>
</tr>
<tr>
<td>pptp-vpn</td>
<td>Specifies the protocol type as PPTP VPN. Configures TCP port 1723.</td>
</tr>
<tr>
<td>sip</td>
<td>Specifies the protocol type as SIP. Configures TCP port 5060 and UDP port 5060.</td>
</tr>
<tr>
<td>ssh</td>
<td>Specifies the protocol type as SSH. Configures TCP port 20</td>
</tr>
<tr>
<td>tls-vpn</td>
<td>Specifies the protocol type as TLS VPN. Configures TCP port 443.</td>
</tr>
<tr>
<td>port &lt;0-65535&gt; [closed</td>
<td>open</td>
</tr>
<tr>
<td></td>
<td>• closed – Specifies that the port(s) is/are closed</td>
</tr>
<tr>
<td></td>
<td>• open – Specifies that the port(s) is/are open</td>
</tr>
<tr>
<td></td>
<td>• unknown – Specifies that the port(s) status is not known</td>
</tr>
</tbody>
</table>

Note: When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.

- connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]

<table>
<thead>
<tr>
<th>connection-capability</th>
<th>Configures the connection capability element in this passpoint policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-protocol &lt;0-255&gt;</td>
<td>Identifies the IP protocol by the protocol’s number. For example, for simple message protocol (SMP) specify 121.</td>
</tr>
</tbody>
</table>
### Examples

```
rfs4000-229D58(config-passpoint-policy-test)#connection-capability 1 ip-protocol 2 port 10 closed
rfs4000-229D58(config-passpoint-policy-test)#show context hotspot2-policy test
  access-network-type chargeable-public
  connection-capability ip-protocol 2 port 10 closed
  3gpp mcc 310 mnc 970
  3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the configured connection capability element on the passpoint policy</td>
</tr>
</tbody>
</table>
27.1.4 domain-name

Indicates the RF Domain(s) that are returned in response to an ANQP query.

Supported platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax
domain-name <DOMAIN-NAME>

Parameters
- domain-name <DOMAIN-NAME>

Examples
rfs4000-229D58(config-passpoint-policy-test)#domain-name TechPubs
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
  access-network-type chargeable-public
  connection-capability ip-protocol 2 port 10 closed
  domain-name TechPubs
  3gpp mcc 310 mnc 970
  3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands
- no
  Removes the RF Domain mapped to this passpoint policy.

Note: An hotspot can be applied across multiple RF Domains.
27.1.5 hessid

Configures the Homogeneous Extended Service Set Identifier (HESSID) for the hotspot. The HESSID uniquely identifies a hotspot provider within a zone. This is essential in zones (such as an airport or shopping mall) having multiple hotspot service providers with overlapping coverage.

An HESSID is a 6 (six) byte identifier that uniquely identifies a set of APs belonging to the same network and exhibiting same network behavior. It is the BSSID (MAC address) of one of the devices (AP) in the zone. When not configured, the radio’s BSSID is used as the HESSID.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax
hessid <MAC>

Parameters
- hessid <MAC>

Examples
rfs4000-229D58(config-passpoint-policy-test)#hessid 00-23-68-88-0D-A7
rfs4000-229D58(config-passpoint-policy-test)#show context hotspot2-policy test
access-network-type chargeable-public
connection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
hessid 00-23-68-88-0D-A7
3gpp mcc 310 mnc 970
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

| no | Removes the HESSID configured with this passpoint policy and reverts back to using the radio’s BSSID |
27.1.6 internet

Advertises the availability of Internet access on this hotspot. The Internet bit in the hotspot's beacon and probe responses indicates if Internet access is available or not. By default this feature is enabled.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax
internet

Parameters
None

Examples
rfs4000-229D58(config-passpoint-policy-test)#internet
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes Internet access on this passpoint policy</td>
</tr>
</tbody>
</table>
### 27.1.7 ip-address-type

*passpoint-policy*

Advertises the IP address type used in this hotspot. This information is returned in response to ANQP queries.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

```plaintext
ip-address-type [ipv4|ipv6]

ip-address-type ipv4 [double-nat|not-available|port-restricted|
not-available|port-restricted-single-nat|public|single-nat|unknown]

ip-address-type ipv6 [available|not-available|unknown]
```

**Parameters**

- **ip-address-type ipv4** [double-nat|not-available|port-restricted|port-restricted-double-nat|port-restricted-single-nat|public|single-nat|unknown]
  - `ip-address-type ipv4` Configures the IPv4 address type availability information
  - `double-nat` Specifies double NATed private IPv4 address is available
  - `not-available` Specifies IPv4 address is not available
  - `port-restricted` Specifies port-restricted IPv4 address is available
  - `port-restricted-double-nat` Specifies port-restricted IPv4 address and double NATed IPv4 address is available
  - `port-restricted-single-nat` Specifies port-restricted IPv4 address and single NATed IPv4 address is available
  - `public` Specifies public IPv4 address is available
  - `single-nat` Specifies single NATed IPv4 address is available
  - `unknown` Specifies no information configured regarding the IPv4 address availability

- **ip-address-type ipv6** [available|not-available|unknown]
  - `ip-address-type ipv6` Configures the IPv6 address type availability information
  - `available` Specifies IPv6 address is available
  - `not-available` Specifies IPv6 address is not available
  - `unknown` Specifies no information configured regarding the IPv6 address availability
Examples
rfs4000-229D58(config-passpoint-policy-test)#ip-address-type ipv6 available

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
access-network-type chargeable-public
collection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
hessid 00-23-68-88-0D-A7
ip-address-type ipv6 available
3gpp mcc 310 mnc 970
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the IP address type configured for this passpoint policy</td>
</tr>
</tbody>
</table>
27.1.8 nai-realm

A Network Access Identifier (NAI) realm element in the passpoint policy identifies a hotspot service provider by the unique NAI realm name.

The following table lists NAI realm configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>nai-realm</td>
<td>Creates a NAI realm name for this hotspot and enters its configuration mode</td>
<td>page 27-14</td>
</tr>
<tr>
<td>nai-realm-config-mode commands</td>
<td>Invokes the NAI realm configuration mode commands</td>
<td>page 27-15</td>
</tr>
</tbody>
</table>
27.1.8.1 nai-realm

Configures a NAI realm name and enters its configuration mode. The NAI realm name identifies the accessible hotspot service providers. You can configure a list of NAI realm names of service providers operating within a specific hotspot zone. This NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query. The configured NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax
nai-realm <HOTSPOT2-NAI-REALM-NAME>

Parameters
- nai-realm <HOTSPOT2-NAI-REALM-NAME>

Examples
rfs4000-229D58(config-passpoint-policy-test)#nai-realm mail.example.com
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#?

Hotspot2 NAI Realm Mode commands:
- eap-method Set an eap method
- no Negate a command or set its defaults
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

Related Commands

no Removes the NAI realm name configured for this passpoint policy
27.1.8.2 nai-realm-config-mode commands

The following table summarizes NAI realm configuration mode commands:

Table 27.3 NAI-Realm-Config-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap-method</td>
<td>Specifies the <em>Extensible Authentication Protocol</em> (EAP) authentication mechanisms supported by each of the service providers associated with this passpoint policy</td>
<td>page 27-16</td>
</tr>
</tbody>
</table>
### 27.1.8.2.1 eap-method

#### nai-realm-config-mode commands

Specifies the EAP authentication mechanisms supported by each of the service providers associated with this passpoint policy.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

#### Syntax

```
eap-method <1-10> [ <1-255> | fast | gtc | identity | ikev2 | ms-auth | mschapv2 | opt | peap | psk | rsa-public-key | sim | tls | ttls ] auth-param [ credential | expanded-eap | expanded-inner-eap | inner-eap | non-eap-inner | tunn-eap-credential | vendor ] [ cert | hw-token | nfc-secure-elem | none | sim | soft-token | username-password | usim | vendor ]
```

#### Parameters

- `eap-method <1-10>` Creates an EAP authentication method and assigns it an index number.
  - `<1-10>` – Specify a identifier for this EAP method from 1 - 10.
  - **Note:** A maximum of 10 (ten) authentication methods can be specified for every NAI realm. After creating the EAP authentication method, specify the associated authentication mechanisms (method types).

- `<1-255>` Identifies the EAP authentication method type from the corresponding Internet Assigned Numbers Authority (IANA) number.
  - **Note:** `<1-255>` – Specify the IANA identity number for the authentication protocol from 1 - 255.

- `fast` Specifies the EAP authentication method type as **Flexible Authentication via Secure Tunneling** (FAST).

- `gtc` Specifies the EAP authentication method type as **Generic Token Card** (GTC).

- `identity` Specifies the EAP authentication method type as **Identification**.

- `ikev2` Specifies the EAP authentication method type as **Internet Key Exchange Protocol version 2** (IKEv2).

- `ms-auth` Specifies the EAP authentication method type as **Microsoft Authentication** (MS-Auth).

- `mschapv2` Specifies the EAP authentication method type as **Microsoft Challenge Handshake Authentication Protocol version 2** (MSCHAPv2).

- `opt` Specifies the EAP authentication method type as **One Time Password** (OTP).

- `peap` Specifies the EAP authentication method type as **Protected Extensible Authentication Protocol** (PEAP).

- `psk` Specifies the EAP authentication method type as **Pre-shared Key** (PSK).

- `rsa-public-key` Specifies the EAP authentication method type as RSA public key protocol.

- `sim` Specifies the EAP authentication method type as **GSM Subscriber Identity Module** (SIM).
The following examples show four EAP authentication methods associated with the NAI realm ‘mail.example.com’. Each method supports a different EAP authentication mechanism:

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-method 1
  tls auth-param vendor hex 00001E
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-method 2
  ttls auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-method 4
  peap auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#show context
  nai-realm mail.example.com
  eap-method 1 tls auth-param vendor hex 00121F
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
27.1.9 net-auth-type

Configure the network authentication type used in this hotspot. The details configured are returned in response to an ANQP query.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax

```
network-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url <URL>}
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-terms</td>
<td>Enables user acceptance of terms and conditions</td>
</tr>
<tr>
<td>dns-redirect</td>
<td>Enables DNS redirection of user</td>
</tr>
<tr>
<td>http-redirect</td>
<td>Enables HTTP redirection of user</td>
</tr>
<tr>
<td>online-enroll</td>
<td>Enables online user enrolment</td>
</tr>
</tbody>
</table>

Examples

```
rfs4000-229D58(config-passpoint-policy-test)#net-auth-type accept-terms url "www.test.com"
rfs4000-229D58(config-passpoint-policy-test)#
```

```
rfs4000-229D58(config-passpoint-policy-test)#show context hotspot2-policy test
access-network-type chargeable-public
connection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
hessid 00-22-68-88-0D-A7
ip-address-type ipv6 available
nai-realm mail.example.com
eap-method 1 ttls auth-param vendor hex 00001E
eap-method 2 rsa-public-key auth-param credential cert
eap-method 3 otp auth-param credential username-password
eap-method 4 peap auth-param credential cert
nai-realm mail.testrealm.com
net-auth-type accept-terms url www.test.com
3gpp mcc 310 mnc 970
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

```
no
```

Removes the network authentication type configured with this passpoint policy.
27.1.10 no

*passpoint-policy*

Removes or reverts the passpoint policy settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

```
no [3gpp|access-network-type|connection-capability|domain-name|hessid|internet|
ip-address-type|nai-realm|net-auth-type|operator|osu|roam-consortium|venue|
wan-metrics]
```

**Parameters**
- **no** `<PARAMETERS>`

<table>
<thead>
<tr>
<th>no <code>&lt;PARAMETERS&gt;</code></th>
<th>Removes or reverts the passpoint policy settings</th>
</tr>
</thead>
</table>

**Examples**

The following example shows the passpoint policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
  access-network-type chargeable-public
  connection-capability ip-protocol 2 port 10 closed
  domain-name TechPubs
  hessid 00-23-68-88-0D-A7
  ip-address-type ipv6 available
  nai-realm mail.example.com
  eap-method 1 tls auth-param vendor hex 00001E
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
  nai-realm mail.testrealm.com
  net-auth-type accept-terms url www.test.com
  3gpp mcc 310 mnc 970
  3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

```
rfs4000-229D58(config-passpoint-policy-test)#no access-network-type
rfs4000-229D58(config-passpoint-policy-test)#no hessid
rfs4000-229D58(config-passpoint-policy-test)#no nai-realm mail.example.com
rfs4000-229D58(config-passpoint-policy-test)#no 3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#no internet
```

```
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
  connection-capability ip-protocol 2 port 10 closed
  domain-name TechPubs
  no internet
  ip-address-type ipv6 available
  nai-realm mail.testrealm.com
  net-auth-type accept-terms url www.test.com
  3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```
27.11 operator

> passpoint-policy

Configures the operator friendly name for this hotspot. The name can be configured in English or in any language other than English. When the name is specified in English, the system allows an ASCII input. If you are using a language other than English, first specify the ISO-639 language code, and then specify the name as an hexadecimal code.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000

Syntax
operator name <OPERATOR-NAME>

Parameters
- operator name <OPERATOR-NAME>

Examples
rfs4000-229D58(config-passpoint-policy-test)#operator name emergencyservices
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
collection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
no internet
ip-address-type ipv6 available
nai-realm mai.testrealm.com
net-auth-type accept-terms url www.test.com
operator name emergencyservices
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

no

Removes the operator friendly name configured for this passpoint policy
27.1.12 osu

The following table lists the OSU SSID/provider configuration commands:

Table 27.4  OSU-SSID/Provider Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>osu</td>
<td>Configures an online sign up (OSU) SSID/provider and enters its configuration mode</td>
<td>page 27-22</td>
</tr>
<tr>
<td>osu-config-mode commands</td>
<td>Summarizes the OSU SSID/provider configuration mode commands</td>
<td>page 27-23</td>
</tr>
</tbody>
</table>
27.1.12.1 osu

Add an online sign up (OSU) SSID (WLAN)/OSU provider and enters its configuration mode

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax

```
 osu [provider <PASSPOINT-OSU-PROVIDER>|ssid <SSID>]
```

Parameters

- osu [provider <PASSPOINT-OSU-PROVIDER>|ssid <SSID>]

Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#?
```

Passpoint OSU Provider Mode commands:
- description Configure the english description of the online signup provider
- icon Add an icon for the online signup provider
- method Specify the online signup method supported by provider
- nai Configure the NAI for the online signup provider
- name Configure the english name of the online signup provider
- no Negate a command or set its defaults
- server-url Configure the signup url for the online signup provider

```
clrscr       Clears the display screen
commit       Commit all changes made in this session
do           Run commands from Exec mode
end          End current mode and change to EXEC mode
exit         End current mode and down to previous mode
help         Description of the interactive help system
revert       Revert changes
service      Service Commands
show         Show running system information
write        Write running configuration to memory or terminal
```

Related Commands

- no | Removes the OSU WLAN/provider configured with this passpoint policy
### osu-config-mode commands

The following table summarizes OSU SSID/provider configuration mode commands:

**Table 27.5  OSU-SSID/Provider-Config-Mode Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Configures the OSU provider’s description</td>
<td>page 27-24</td>
</tr>
<tr>
<td>icon</td>
<td>Adds the OSU provider’s icon</td>
<td>page 27-25</td>
</tr>
<tr>
<td>method</td>
<td>Configures the open sign up methods available on this OSU provider</td>
<td>page 27-26</td>
</tr>
<tr>
<td>nai</td>
<td>Configures the OSU provider’s NAI</td>
<td>page 27-27</td>
</tr>
<tr>
<td>name</td>
<td>Configures the OSU provider’s name</td>
<td>page 27-28</td>
</tr>
<tr>
<td>no</td>
<td>Removes the settings configured for this OSU provider</td>
<td>page 27-29</td>
</tr>
<tr>
<td>server-url</td>
<td>Configures the OSU provider server’s URL</td>
<td>page 27-30</td>
</tr>
</tbody>
</table>
27.1.12.2.2 description

osu-config-mode commands

Configures the OSU SSID/provider’s description. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax

description [description | iso-lang <ISO-LANG-CODE>]

Parameters
- **description [description | iso-lang <ISO-LANG-CODE>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Provides a description for the OSU provider. It should not exceed 253 characters in length.</td>
</tr>
<tr>
<td>iso-lang &lt;ISO-LANG-CODE&gt;</td>
<td>Identifies the language by its ISO 639 language code (for example, ‘chi-chinese’ or ‘spa-spanish’). By default the language is set to English. If specifying the description in any language other than English, specify the ISO language code.</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)# description "Provides free service for testing purposes"
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)# show context osu provider WiFi
  description "Provides free service for testing purposes"
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

- **no** Removes this OSU provider’s description
27.12.2.3 icon

**osu-config-mode commands**

Adds the OSU provider’s icon. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

```
icon iso-lang <ISO-LANG-CODE> width <0-65535> height <0-65535>
  mime-type <FILE-MIME-TYPE> file [<IMAGE-FILENAME/PATH>|<FILE-NAME>]
```

**Parameters**

- **icon iso-lang <ISO-LANG-CODE> width <0-65535> height <0-65535> mime-type <FILE-MIME-TYPE> file [<IMAGE-FILENAME/PATH>|<FILE-NAME>]**
  - **icon iso-lang <ISO-LANG-CODE>** — Configures an icon representing the OSU provider
    - **<ISO-LANG-CODE>** – Identifies the language by its ISO 639 language code (for example, ‘chi-chinese’ or ‘spa-spanish’). By default the language is set to English. If specifying the image file name and path in any language other than English, specify the ISO language code.
  - **width <0-65535>** — Configures the icon’s width in pixels
    - **<0-65535>** – Specify a value from 0 - 65535 pixels.
  - **height <0-65535>** — Configures the icon’s height in pixels
    - **<0-65535>** – Specify a value from 0 - 65535 pixels.
  - **mime-type <FILE-MIME-TYPE>** — Configures a string describing the icon’s standard mime type. For example, image/png
    - **<FILE-MIME-TYPE>** – Specify the icon’s mime type.
  - **file [<IMAGE-FILENAME/PATH>|<FILE-NAME>]** — Configures the location and name of the image file
    - **<IMAGE-FILENAME/PATH>|<FILE-NAME>** – Specify the path and filename. For example, flash:/icon.png
    - **<FILE-NAME>** – Use this option to specify the filename in the flash:/ directory

**Examples**

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#icon iso-lang eng
  width 128 height 128 mime-type image/png file flash:/wifi_icon

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
  osu provider WiFi
description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

**Related Commands**

- **no** — Removes this OSU provider’s icon
27.1.12.2.4 method

osu-config-mode commands

Configures the open sign up methods available on this OSU provider. This value is returned, in the specified order of precedence, in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax

method [oma-dm|soap-xml-spp] priority <1-2>

Parameters

- method [oma-dm|soap-xml-spp] priority <1-2>

Configure the online sign up methods supported by this OSU provider.

- oma-dm – Configures the OSU method used as Open Mobile Alliance (OMA) device management
- soap-xml-spp – Configures the OSU method used as Soap-xml subscription provisioning protocol
- priority <1-2> – Sets the priority of the specified method. Select a value from 1 - 2. The default is one (1).

Examples

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#method soap-xml-spp priority 1

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context osu provider WiFi
description "Provides free service for testing purposes"
icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
method soap-xml-spp priority 1

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#

Related Commands

no

Removes the online sign up methods configured on this OSU provider
27.12.2.5 nai

**osu-config-mode commands**

Configures the OSU provider’s NAI. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

nai <WORD>

**Parameters**

- nai <WORD>

<table>
<thead>
<tr>
<th>nai &lt;WORD&gt;</th>
<th>Configures the OSU provider’s NAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>- Specify the NAI.</td>
</tr>
</tbody>
</table>

**Examples**

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#nai wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context osu provider WiFi
description "Provides free service for testing purposes"
icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
method soap-xml-spp priority 1
nai wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#

**Related Commands**

| no | Removes this OSU provider’s NAI |
27.12.2.6 name

*osu-config-mode commands*

Configures the OSU provider’s name. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

```
name [NAME|iso-lang ISO-LANG-CODE]
```

**Parameters**

- name [NAME|iso-lang ISO-LANG-CODE]

<table>
<thead>
<tr>
<th>NAME</th>
<th>Configures the OSU provider’s name. It should not exceed 253 characters in length.</th>
</tr>
</thead>
<tbody>
<tr>
<td>iso-lang</td>
<td>Identifies the language by its ISO 639 language code (for example, ‘chi-chinese’ or ‘spa-spanish’). By default the language is set to English. If specifying the name in any language other than English, specify the ISO language code.</td>
</tr>
</tbody>
</table>

**Examples**

```
x9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#name "WIFI Alliance OSU"
x9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
  osu provider WIFI
    name "WIFI Alliance OSU"
    description "Provides free service for testing purposes"
    icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
    method soap-xml-spp priority 1
    nai wifi.org
```

**Related Commands**

- `no` Removes this OSU provider’s name
27.1.12.2.7 no

- **osu-config-mode commands**

Removes the settings configured for this OSU provider. Once removed the information is not included in the ANQP providers list.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

no [description|icon|method|nai|name|server-url]

no [description|icon|name] {iso-lang <ISO-LANG-CODE>}

no [nai|server-url]

no method [oma-dm|soap-xml-spp]

**Parameters**

- no <PARAMETERS>

```
no <PARAMETERS> Removes the settings configured for this OSU provider
```

**Examples**

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context osu provider WiFi
   name "WIFI Alliance OSU"
   description "Provides free service for testing purposes"
   icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
   method soap-xml-spp priority 1
   nai wifi.org
   server-url osu-server.wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#no description
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#no icon iso-lang eng
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#no name
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context osu provider WiFi
   method soap-xml-spp priority 1
   nai wifi.org
   server-url osu-server.wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```
### 27.1.12.2.8 server-url

**osu-config-mode commands**

Configures the OSU provider server’s URL. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

```
server-url <URL>
```

**Parameters**

- `server-url <URL>`

**Examples**

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#server-url
osu-server.wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
osu provider WiFi
   name "WIFI Alliance OSU"
   description "Provides free service for testing purposes"
   icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
   method soap-xml-spp priority 1
   nai wifi.org
   server-url osu-server.wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

**Related Commands**

```
no
```

Removes this OSU provider’s server’s URL.
27.1.13 roam-consortium

> passpoint-policy

Configures a list of Roaming Consortium (RC) Organization Identifiers (OIs) supported on this hotspot. The beacons and probe responses communicate this Roaming Consortium list to devices. This information enables a device to identify the networks available through this AP.

Each OI identifies a either a group of Subscription Service Providers (SSPs) or a single SSP.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax
roam-consortium hex <WORD>

Parameters
- roam-consortium hex <WORD>

<table>
<thead>
<tr>
<th>roam-consortium hex &lt;WORD&gt;</th>
<th>Adds a Roaming Consortium OI to this hotspot in hexadecimal format</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>hex &lt;WORD&gt;</th>
<th>Configures a hexadecimal input</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)</td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58(config-passpoint-policy-test)#roam-consortium hex 223344

rfs4000-229D58(config-passpoint-policy-test)#show context hotspot2-policy test
connection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
no internet
ip-address-type ipv6 available
nai-realm mai.testrealm.com
net-auth-type accept-terms url www.test.com
operator name emergencyservices
roam-consortium hex 223344
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands
- no

Removes the Roaming Consortium OIs supported on this passpoint policy
27.1.14 venue

Configures the venue where this hotspot is located. The hotspot venue configuration informs prospective clients about the hotspot’s nature of activity, such as educational, institutional, residential etc.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

Syntax

venue [group|name]

venue group [assembly|business|educational|industrial|institutional|mercantile|
           outdoor|residential|storage|unspecified|utility-and-misc|vehicular] type

venue name [<VENUE-NAME>|iso-lang]
venue name <VENUE-NAME>
venue name iso-lang <ISO-LANG-CODE> <VENUE-NAME>

Parameters
- venue group [assembly|business|educational|industrial|institutional|mercantile|
              outdoor|residential|storage|unspecified|utility-and-misc|vehicular] type
- type – Specifies the venue type for this group. The options are:
  - <0-255> – Specifies an unlisted venue type number from 0 -255
  - amphitheater – Specifies the venue type as amphitheater (4)
  - amusement-park – Specifies the venue type as amusement park (5)
  - arena – Specifies the venue type as arena (1)
  - bar – Specifies the venue type as bar (12)
  - coffee-shop – Specifies the venue type as a coffee shop (13)
  - convention-centre – Specifies the venue type as a convention center (7)
  - emergency-coordination-center – Specifies the venue type as an emergency coordination center (15)
  - library – Specifies the venue type as a library (8)
  - museum – Specifies the venue type as a museum (9)
  - passenger-terminal – Specifies the venue type as a passenger terminal (3)
  - place-of-worship – Specifies the venue type as a place of worship (6)
  - restaurant – Specifies the venue type as a restaurant (10)
  - stadium – Specifies the venue type as a stadium (2)
  - theater – Specifies the venue type as a theater (11)
  - unspecified – Specifies the venue type as not specified (0)
  - zoo – Specifies the venue type as a zoo (14)
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Hotspot Types</th>
</tr>
</thead>
</table>
| business type | Configures the venue group as business (2). This hotspot type is applicable to business venues. | - type – Specifies the venue type for this group. The options are:  
  - `<0-255>` – Specifies an unlisted venue type number from 0 - 255  
  - attorney – Specifies the venue type as the attorney’s office (9)  
  - bank – Specifies the venue type as a bank (2)  
  - doctor – Specifies the venue type as a doctor or dentist’s office (1)  
  - fire-station – Specifies the venue type as a fire station (3)  
  - police-station – Specifies the venue type as a police station (4)  
  - post-office – Specifies the venue type as a post office (5)  
  - professional-office – Specifies the venue type as a professional office (7)  
  - research-and-development-facility – Specifies the venue type as a research facility (8)  
  - unspecified – Specifies the venue type as not specified (0) |
| educational | Configures the venue group as educational (3). This hotspot type is applicable to educational institutions. | - type – Specifies the venue type for this group. The options are:  
  - `<0-255>` – Specifies an unlisted venue type number from 0 - 255  
  - school-primary – Specifies the venue type as a primary school (1)  
  - school-secondary – Specifies the venue type as a secondary school (2)  
  - university – Specifies the venue type as a university or college (3)  
  - unspecified – Specifies the venue type as not specified (0) |
| industrial | Configures the venue group as industrial (4). This hotspot type is applicable to industrial venues. | - type – Specifies the venue type for this group. The options are:  
  - `<0-255>` – Specifies an unlisted venue type number from 0 - 255  
  - factory – Specifies the venue type as a factory (1)  
  - unspecified – Specifies the venue type as not specified (0) |
| institutional | Configures the venue group as institutional (4). This hotspot type is applicable to public health and other institutions. | - type – Specifies the venue type for this group. The options are:  
  - `<0-255>` – Specifies an unlisted venue type number from 0 - 255  
  - group-home – Specifies the venue type as a group-home (4)  
  - hospital – Specifies the venue type as a hospital (1)  
  - long-term-care – Specifies the venue type as a long term care facility (2)  
  - prison – Specifies the venue type as a prison or jail (5)  
  - rehab – Specifies the venue type as a rehabilitation facility (3)  
  - unspecified – Specifies the venue type as not specified (0) |
| mercantile | Configures the venue group as mercantile (6). This hotspot type is applicable to public mercantile venues. | - type – Specifies the venue type for this group. The options are:  
  - `<0-255>` – Specifies an unlisted venue type number from 0 - 255  
  - automotive – Specifies the venue type as a automotive service center (3)  
  - gas-station – Specifies the venue type as a gas station (5)  
  - grocery – Specifies the venue type as a grocery store (2)  
  - mall – Specifies the venue type as a shopping mall (4)  
  - retail – Specifies the venue type as a retail store (1)  
  - unspecified – Specifies the venue type as not specified (0) |
<table>
<thead>
<tr>
<th>Venue Type</th>
<th>Description</th>
<th>Configuration Details</th>
</tr>
</thead>
</table>
| **outdoor** | Configures the venue group as outdoor (11). This hotspot type is applicable to public outdoor venues. | • type – Specifies the venue type for this group. The options are:  
  • <0-255> – Specifies an unlisted venue type number from 0 -255  
  • bus-stop – Specifies the venue type as a bus stop (5)  
  • city-park – Specifies the venue type as a city park (2)  
  • kiosk – Specifies the venue type as a kiosk (6)  
  • muni-mesh – Specifies the venue type as a muni-mesh (municipal wireless Wi-Fi) (1)  
  • rest-area – Specifies the venue type as a rest area (3)  
  • traffic-control – Specifies the venue type as a traffic control area (4)  
  • unspecified – Specifies the venue type as not specified (0) |
| **residential** | Configures the venue group as residential (7). This hotspot type is applicable to residential complexes. | • type – Specifies the venue type for this group. The options are:  
  • <0-255> – Specifies an unlisted venue type number from 0 -255  
  • boarding-house – Specifies the venue type as a boarding-house (4)  
  • dorm – Specifies the venue type as a dormitory (3)  
  • hotel – Specifies the venue type as a hotel or motel (2)  
  • private – Specifies the venue type as a private residence (1)  
  • unspecified – Specifies the venue type as not specified (0) |
| **storage** | Configures the venue group as storage (8). This hotspot type is applicable to storage groups. | • type – Specifies the venue type for this group. The options are:  
  • <0-255> – Specifies an unlisted venue type number from 0 -255  
  • unspecified – Specifies the venue type as not specified (0) |
| **unspecified** | Configures the venue group as unspecified (0) | • type – Specifies the venue type for this group. The options are:  
  • <0-255> – Specifies an unlisted venue type number from 0 -255  
  • unspecified – Specifies the venue type as not specified (0) |
| **utility-and-misc** | Configures the venue group as utility and miscellaneous (8) | • type – Specifies the venue type for this group. The options are:  
  • <0-255> – Specifies an unlisted venue type number from 0 -255  
  • unspecified – Specifies the venue type as not specified (0) |
| **vehicular** | Configures the venue group as vehicular (7). This hotspot type is applicable to mobile venues. | • type – Specifies the venue type for this group. The options are:  
  • <0-255> – Specifies an unlisted venue type number from 0 -255  
  • airplane – Specifies the venue type as an airplane (2)  
  • auto – Specifies the venue type as an automobile or truck (1)  
  • bus – Specifies the venue type as a bus (3)  
  • ferry – Specifies the venue type as a ferry (5)  
  • motor-bike – Specifies the venue type as a motor bike (7)  
  • ship – Specifies the venue type as a ship or boat (5)  
  • train – Specifies the venue type as a train (6)  
  • unspecified – Specifies the venue type as not specified (0) |
operator name <VENUE-NAME>

name <WORD> Configures the venue name in English
• <WORD> – Specify the venue name in ASCII format.

operator name iso-lang <ISO-LANG-CODE> <VENUE-NAME>

name iso-lang <ISO-LANG-CODE> <VENUE-NAME> Configures a non-English venue name
• iso-lang <ISO-LANG-CODE> – Identifies the language by its ISO 639 language code (for example, ‘chi-chinese’ or ‘spa-spanish’).
• <ISO-LANG-CODE> – Specify the 3 character iso-639 language code (for example, ‘chi-chinese’ or ‘spa-spanish’).
• <VENUE-NAME> – Specifies the venue name as a hexadecimal code

Examples
rfs4000-229D58(config-passpoint-policy-test)#venue name PublicSchool
rfs4000-229D58(config-passpoint-policy-test)#venue group assembly type coffee-shop
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
connection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
no internet
ip-address-type ipv6 available
nai-realm mai.testrealm.com
net-auth-type accept-terms url www.test.com
operator name emergencyservices
roam-consortium hex 223344
venue group assembly type coffee-shop
venue name PublicSchool
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

no Removes the venue group and type configured with this passpoint policy
27.1.15 `wan-metrics`

*passpoint-policy*

Configures the WAN performance metrics for this hotspot. This command configures the upstream and downstream speeds associated with this hotspot. The upstream and downstream speed values (in Kbps) are estimates of the bandwidth available on the WAN. This information is returned in response to client ANQP query, and is useful for clients having a minimum and/or large bandwidth requirement.

Supported in the following platforms:
- **Access Points** — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX7500, NX7510, NX7520, NX7530, NX9000, NX9600

**Syntax**

```
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>
```

**Parameters**

- `wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>`

<table>
<thead>
<tr>
<th>wan-metrics</th>
<th>Specifies the WAN metrics for the up and down traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>down-speed</td>
<td>Configures the downstream traffic speed</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>• &lt;0-4294967295&gt; – Specify a value from 0 - 4294967295 Kbps.</td>
</tr>
<tr>
<td>up-speed</td>
<td>Configures the upstream traffic speed</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>• &lt;0-4294967295&gt; – Specify a value from 0 - 4294967295 Kbps.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-passpoint-policy-test)#wan-metrics down-speed 2000 up-speed 2000
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
connection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
no internet
ip-address-type ipv6 available
nai-realm mai.testrealm.com
net-auth-type accept-terms url www.test.com
operator name emergencyservices
roam-consortium hex 223344
venue group assembly type coffee-shop
venue name PublicSchool
wan-metrics down-speed 2000 up-speed 2000
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

**Related Commands**

- `no` | Removes the WAN metrics configuration on this passpoint policy
CHAPTER 28
BORDER GATEWAY PROTOCOL

This chapter summarizes the Border Gateway Protocol (BGP) related configuration commands in the CLI command structure.

BGP is a routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing information between Autonomous Systems (ASs) on the Internet. The routing information shared includes details, such as ASs traversed to a particular destination, reachable ASs, best paths available, network policies and rules applied on a route etc. These details appear as BGP attributes carried in routing update packets. BGP uses this information to make routing decisions. Therefore, the primary role of a BGP system is to exchange routing information with other BGP peers.

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a graceful close (all outstanding data is delivered before the connection is closed). Routing information exchanged through BGP supports only destination-based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

An AS is a set of routers under the same administration that use Interior Gateway Protocol (IGP) and common metrics to define how to route packets within the AS. There are two types of BGP systems: external BGP (eBGP) and internal BGP (iBGP). iBGP represents the exchange of routing information between BGP peers within an AS. Whereas, when two BGP peers, belonging to different ASs, are connected you have an eBGP setup.

BGP peers (also referred to as neighbors) are BGP enabled devices that are directly connected through an established TCP connection. When two BGP enabled peers establish a TCP connection the first time, they exchange their BGP routing tables. All subsequent route table modifications are exchanged as route updates. BGP tracks these route updates by maintaining route table version numbers. With every update the version number changes. At any given point in time, all BGP peers should have the same route table version. The peer-to-peer TCP connections are kept alive through keepalive packets exchanged at specified intervals. Errors and special events are communicated between peers as notification packets.

This chapter is organized as follows:

- `bgp-ip-prefix-list-config commands`
- `bgp-ip-access-list-config commands`
- `bgp-as-path-list-config commands`
- `bgp-community-list-config commands`
- `bgp-extcommunity-list-config commands`
- `bgp-route-map-config commands`
- `bgp-router-config commands`
- `bgp-neighbor-config commands`
NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
28.1 bgp-ip-prefix-list-config commands

IP prefix lists are a convenient way to filter prefixes (contained in route update packets) transmitted to (or received from) other BGP supported routers. IP prefix lists are similar to access lists. They contain ordered entries (deny or permit prefix rules), identified by their sequence numbers. Each rule specifies match criteria (network and subnet prefixes and prefix masks) to match. When a prefix (received or transmitted) matches the prefix specified in one of the rules, it is filtered and an action is applied depending on where the IP prefix list is used. For example, when used in the BGP neighbor context, the prefixes received from the neighbor are filtered and the filtered prefixes are either rejected or accepted depending on the rule type (deny or permit).

IP prefix lists are also used in the BGP route map context to filter prefixes. The action applied, on filtered prefixes is set within the route map. Another use case for IP prefix lists is to filter prefixes before redistribution of local OSPF routes to eBGP enabled ASs.

Like in access lists, these deny and permit prefix rules are processed sequentially, in ascending order of their sequence number. Once a match is made, the BGP enabled router stops processing all subsequent rules in the ip-prefix-list.

IP prefix lists are used as match criteria in the following contexts:

- BGP neighbor. For more information, see use.
- BGP route-map context. For more information, see match.

To navigate to the ip-prefix-list configuration instance, use the following command:

```
<DEVICE>(config)#bgp ip-prefix-list <IP-PREFIX-LIST-NAME>
```

BGP IP Prefix List Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>IP Prefix deny rule to specify packets to reject</td>
<td>page 28-4</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td></td>
</tr>
<tr>
<td>permit</td>
<td>IP Prefix permit rule to specify packets to forward</td>
<td></td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td></td>
</tr>
<tr>
<td>commit</td>
<td>Commit all changes made in this session</td>
<td></td>
</tr>
<tr>
<td>do</td>
<td>Run commands from Exec mode</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td></td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td></td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td></td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal</td>
<td></td>
</tr>
</tbody>
</table>

The following table summarizes the BGP IP prefix list configuration commands:

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates and configures a deny prefix-list rule</td>
<td>page 28-4</td>
</tr>
<tr>
<td>permit</td>
<td>Creates and configures a permit prefix-list rule</td>
<td>page 28-5</td>
</tr>
<tr>
<td>no</td>
<td>Removes the specified deny or permit prefix-list rule from this IP prefix list</td>
<td>page 28-6</td>
</tr>
</tbody>
</table>
```
### 28.1.1 deny

**bgp-ip-prefix-list-config commands**

Creates and configures a deny prefix-list rule. The deny rule specifies match criteria based on which prefixes received from (or transmitted to) a BGP neighbor are filtered. A deny action is applied on these filtered prefixes. For example, in the BGP router neighbor context a filter is applied using a IP prefix list. The list contains a deny rule with a prefix to match as 192.168.13.0/24. All prefixes received from the neighbor matching this prefix are denied.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
deny prefix-list <1-4292967294> \[<PREFIX-TO-MATCH/MASK>|any\]
deny prefix-list <1-4292967294> \[<PREFIX-TO-MATCH/MASK> {ge <0-32>|le <0-32>} |any\]
```

**Parameters**

- **deny prefix-list <1-4292967294> \[<PREFIX-TO-MATCH/MASK>\]any\]**
  - <1-4294967295> — Configures a sequence number for this deny rule. Specify a value from 1 - 4294967295. Within a prefix list, rules are applied in an ascending order of their sequence number. Rules with lower sequence number are applied first.
  - <PREFIX-TO-MATCH/MASK> — Specify the prefix to match. For example 10.0.0.0/8 or 192.168.13.0/24. Routes matching the specified prefix are filtered.
    - ge <0-32> — Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask)
    - le <0-32> — Optional. Specifies a less than or equal to value for the IP prefix length

**Note:** The ‘ge’ and ‘le’ options specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria.

- any — Sets the prefix match criteria to any. When selected, all routes are filtered, and the action applied is deny. At the backend, this option sets the match criteria to 0.0.0.0/0 le 32.

**Examples**

```plaintext
nx9500-6C8809(config-bgp-ip-prefix-list-test)#deny prefix-list 1 168.192.13.0/24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
  deny prefix-list 1 168.192.13.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th><strong>no</strong></th>
<th>Removes a deny prefix-list rule from this IP prefix list</th>
</tr>
</thead>
</table>
### 28.1.2 permit

**bgp-ip-prefix-list-config commands**

Creates and configures a permit prefix-list rule. The permit rule specifies match criteria based on which prefixes received from (or transmitted to) a BGP neighbor are filtered. A permit action is applied on these filtered prefixes. For example, in the BGP router neighbor context a filter is applied using an IP prefix list. The list contains a permit rule with a prefix to match as 172.168.10.0/24. All prefixes received from the neighbor matching this prefix are permitted.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]
```

**Parameters**

- `permit prefix-list <1-4294967295>`: Creates a sequence number for this permit rule. Specify a value from 1 - 4294967295. Within a prefix list, rules are applied in an ascending order of their sequence number. Rules with lower sequence number are applied first.
- `<PREFIX-TO-MATCH/MASK>`: Specify the prefix to match. For example 10.0.0.0/8 or 192.168.13.0/24. Routes matching the specified prefix are filtered.
  - `ge`: Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask)
  - `le`: Optional. Specifies a less than or equal to value for the IP prefix length

**Note:** Use the `ge` and `le` options to specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria.

- `any`: Sets the prefix match criteria to any. When selected, all routes are filtered, and the action applied is permit. At the backend, this option sets the match criteria to `0.0.0.0/0 le 32`.

**Examples**

```bash
nx9500-6C8809(config-bgp-ip-prefix-list-test)#permit prefix-list 2 172.122.10.0/24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
  deny prefix-list 1 168.192.13.0/24
  permit prefix-list 2 172.122.10.0/24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

**Related Commands**

- `no`: Removes a permit prefix rule from this IP prefix list
28.1.3 no

* bgp-ip-prefix-list-config commands

Removes the specified deny or permit prefix-list rule from this IP prefix list

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [deny|permit]

no [deny|permit] prefix-list <1-4294967295> {<PREFIX-TO-MATCH/MASK>|any}
```

**Parameters**

- `no <PARAMETERS>`

| no <PARAMETERS> | Removes a deny or permit rule from this IP prefix list |

**Examples**

The following example shows the IP prefix list 'test' settings before the 'no' command is executed:

```plaintext
nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
deny prefix-list 1 168.192.13.0/24
permit prefix-list 2 172.122.10.0/24
```

The following example shows the IP prefix list 'test' settings after the 'no' command is executed:

```plaintext
nx9500-6C8809(config-bgp-ip-prefix-list-test)#no deny prefix-list 1 168.192.13.0/24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
  permit prefix-list 2 172.122.10.0/24
```

nx9500-6C8809(config-bgp-ip-prefix-list-test)#
28.2 bgp-ip-access-list-config commands

BORDER GATEWAY PROTOCOL

BGP peers and route maps can reference a single IP based access control list (ACL). Apply IP ACLs to both inbound and outbound route updates. When applied to a BGP enabled router, every route update is passed through the ACL. Each ACL contains deny and permit entries that are applied sequentially, in the order they appear within the list. When a route matches an entry, the decision to permit or deny the route is applied. Once a match is made the remaining entries in the ACL are not processed.

BGP IP ACLs are used as match criteria in the following contexts:

- BGP neighbor. For more information, see `use`.
- BGP route-map context. For more information, see `match`.

To navigate to the BGP IP ACL configuration instance, use the following command:

```
<DEVICE>(config)#bgp ip-access-list <IP-ACL-NAME>
```

BGP IP Access List Mode commands:
- `deny` Specify packets to reject
- `no` Negate a command or set its defaults
- `permit` Specify packets to forward
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

The following table summarizes the BGP IP access list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deny</code></td>
<td>Creates and configures a deny entry rule for this BGP IP ACL</td>
<td>page 28-8</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Creates and configures a permit entry for this BGP IP ACL</td>
<td>page 28-9</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Removes a deny or permit entry from this BGP IP ACL</td>
<td>page 28-10</td>
</tr>
</tbody>
</table>
## 28.2.1 deny

### bgp-ip-access-list-config commands

Creates and configures a deny entry for this BGP IP ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

### Syntax

deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]

### Parameters

- **deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]**

| deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any] | Creates and configures a deny entry for this BGP IP ACL
|-------------------------------------------------------------|
| [<PREFIX-TO-MATCH/MASK> {exact-match}|any] | - Specify the prefix to match.
| exact-match | - Optional. Enables an exact match of the prefix provided in the previous step. When configured, the route is denied only in case of an exact match.
| any | - Specifies the prefix to match as 'any'.

### Examples

nx9500-6C8809(config-bgp-ip-access-list-test)#deny access-list 192.168.13.0/24 exact-match

nx9500-6C8809(config-bgp-ip-access-list-test)#show context bgp ip-access-list test
deny access-list 192.168.13.0/24 exact-match

nx9500-6C8809(config-bgp-ip-access-list-test)#

### Related Commands

| no | Removes the specified the deny entry in this IP BGP ACL |
28.2.2 permit

- **bgp-ip-access-list-config commands**

  Creates and configures a permit entry for this BGP IP ACL

  Supported in the following platforms:

  - Wireless Controllers — RFS4000, RFS6000
  - Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

  **Syntax**

  `permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]`

  **Parameters**

  - `permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]`

  | `permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]` |
  |---------------------------------------------------------------|
  | Creates and configures a permit entry for this BGP IP ACL     |
  | - `<PREFIX-TO-MATCH/MASK>` – Specify the prefix to match.     |
  | - `exact-match` – Optional. Enables an exact match of the prefix provided in the |
  | previous step. When configured, the route is permitted only in case of an exact match. |
  | - `any` – Specifies the prefix to match as ‘any’.             |

  **Examples**

  ```
  nx9500-6C8809(config-bgp-ip-access-list-test)#permit access-list 172.168.10.0/24
  nx9500-6C8809(config-bgp-ip-access-list-test)#show context
  bgp ip-access-list test
  permit access-list 172.168.10.0/24
  deny access-list 192.168.13.0/24 exact-match
  nx9500-6C8809(config-bgp-ip-access-list-test)#
  ```

  **Related Commands**

  - `no` Removes the specified the permit entry in this IP BGP ACL
28.2.3  no

> bgp-ip-access-list-config commands

Removes a deny or permit entry from this BGP IP ACL

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|permit]

no [deny|permit] access-list [<PREFIX-TO-MATCH/MASK>|any]

Parameters

- no <PARAMETERS>

no <PARAMETERS> | Removes a deny or permit entry from this BGP IP ACL

Examples

The following example shows the BGP IP ACL ‘test’ settings before the ‘no’ command is executed:

```
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
  permit access-list 172.168.10.0/24
  deny access-list 192.168.13.0/24 exact-match
```

```
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

```
nx9500-6C8809(config-bgp-ip-access-list-test)#no permit access-list 172.168.10.0/24
```

The following example shows the BGP IP ACL ‘test’ settings after the ‘no’ command is executed:

```
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
  deny access-list 192.168.13.0/24 exact-match
```

```
nx9500-6C8809(config-bgp-ip-access-list-test)#
```
28.3 bgp-as-path-list-config commands

BGP enabled devices use routing updates to exchange network routing information with each other. This information includes route details, such as the network number, path specific attributes, and the list of Autonomous System Numbers (ASNs) that a route traverses to reach a destination. This list is contained in the AS path.

An AS path access control list (ACL) filters AS paths (routes) included in routing updates. Each AS path access list consists of deny and/or permit rules that define regular expressions (match criteria). When configured and applied on inbound and outbound routing updates, the BGP AS path attributes are matched against the regular expressions specified in the AS path ACL. In case of a match, the route is filtered and an action (deny or permit) is applied. Once a match is made subsequent rules in the AS path access list are not processed.

AS path access lists also help prevent looping within an AS. Routing loops are prevented by rejecting routing updates containing local ASNs. Since local ASNs indicate that the route has already traveled through that autonomous system, by rejecting them looping is avoided.

AS path access lists are used as match criteria in the following contexts:

- BGP neighbor. For more information, see use.
- BGP route map context. For more information, see match.

To navigate to the AS path configuration instance, use the following command:

```
<DEVICE>(config)#bgp as-path <AS-PATH-LIST-NAME>
```

The following table summarizes the BGP AS path list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates and configures a deny as-path-list rule</td>
<td>page 28-12</td>
</tr>
<tr>
<td>permit</td>
<td>Creates and configures a permit as-path-list rule</td>
<td>page 28-13</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny or permit rule from this AS path ACL</td>
<td>page 28-14</td>
</tr>
</tbody>
</table>
28.3.1 deny

`bgp-as-path-list-config commands`

Creates and configures a deny as-path-list rule. The deny rule specifies a regular expression to match. This regular expression, a string against the BGP AS paths contained in routing updates. AS paths matching the provided string are filtered and a deny action is applied.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

deny as-path <REG-EXP>

**Parameters**

- deny as-path <REG-EXP>

| deny as-path <REG-EXP> | Configures a match criteria (regular expression).  
|------------------------|---------------------------------------------------|
| <REG-EXP>              | Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule)  

**Note:** Regular expressions are treated as a ‘ASCII string’ and not as a sequence of numbers. Create a regular expression ideally suited to filter the required AS paths.

**Usage Guidelines**

The following table lists some of the characters used in forming regular expressions:

<table>
<thead>
<tr>
<th>Character to use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Indicates the start of a string</td>
</tr>
<tr>
<td>$</td>
<td>Indicates the end of a string</td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>Indicates a comma, left brace, right brace, start and end of an input string, or a space. For example, “_ _”.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
nx9500-6C8809(config-bgp-as-path-list-test)#deny as-path ^100$

nx9500-6C8809(config-bgp-as-path-list-test)#show context bgp as-path-list test
deny as-path ^100$
nx9500-6C8809(config-bgp-as-path-list-test)#
```

**Related Commands**

| no | Removes the specified deny as-path ACL rule |
### 28.3.2 permit

**bgp-as-path-list-config commands**

Creates and configures a permit as-path-list rule. The permit rule specifies a regular expression to match. This regular expression is matched against the BGP AS paths contained in routing updates. AS paths matching the provided string are filtered and a permit action is applied.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit as-path <REG-EXP>
```

**Parameters**

- `permit as-path <REG-EXP>`

**Usage Guidelines**

The following table lists some of the characters used in forming regular expressions:

<table>
<thead>
<tr>
<th>Character to use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Indicates the start of a string</td>
</tr>
<tr>
<td>$</td>
<td>Indicates the end of a string</td>
</tr>
</tbody>
</table>
| _ (underscore)   | Indicates a comma, left brace, right brace, start and end of an input string, or a space. For example, “_ _”.

**Examples**

```plaintext
nx9500-6C8809(config-bgp-as-path-list-test)#permit as-path _200_

nx9500-6C8809(config-bgp-as-path-list-test)#permit as-path _323_

nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
deny as-path ^100$
permit as-path _323_
permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
```

**Related Commands**

- `no` Removes the specified permit as-path ACL rule
28.3.3 no

Removes a deny or permit rule from this AS path ACL

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

no as-path-list [deny|permit] <REG-EXP>

Parameters

- no <PARAMETERS>

Examples

nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
deny as-path ^100$
permit as-path _323_
permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#

nx9500-6C8809(config-bgp-as-path-list-test)#no permit as-path _323_
nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
deny as-path ^100$
permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
28.4 bgp-community-list-config commands

| BORDER GATEWAY PROTOCOL |

Creates and configures a named community list

IP BGP routes have a set of attributes, mandatory and optional. The community and extended community attributes are optional. Optional attributes are specified by network administrators to mark (color) routes received in updates containing these attributes. These marked routes are filtered and special actions applied (accepted, preferred, distributed, or advertised). For example, the NO_EXPORT community, indicates that routes attached to it are local and not to be advertised to external ASs. Similarly, a set of routes using a common routing policy can be tagged to a community, and the policy applied to the community.

A BGP community is a group of routes sharing common attributes. Route updates contain community information in the form of path attributes. These attributes help identify community members.

A BGP community list is a list of deny or permit entries. It is assigned either a name (regular expressions, predefined community names) or a number. Assigning names to communities increases the number of configurable community lists. All rules applicable to numbered communities apply to named communities too. The only difference being in the number of attributes configurable for a named community list.

Since the community attribute is optional, it is shared only between devices that understand communities and are configured to handle communities. By default the community attribute is not sent to neighbors unless the send-community command option is enabled in the BGP neighbor context. For more information see, send-community.

Some of the predefined, globally used communities are:

- **no-export** – Routes tagged to this community are not advertised to external BGP peers
- **no-advertise** – Routes tagged to this community are not advertised to any BGP peers
- **local-as** – Routes tagged to this community are not advertised outside the local AS
- **internet** – Routes tagged to this community are advertised to the internet community. By default all BGP enabled devices belong to this community.

BGP community lists are used in the following context as match clauses:

- BGP route map context. For more information, see match.

To navigate to the BGP community configuration instance, use the following command:

```
<DEVICE>(config)#bgp community-list <COMMUNITY-LIST-NAME>
```

```
<DEVICE>(config-bgp-community-list-<COMMUNITY-LIST-NAME>)#?
```

BGP Community List Mode commands:

```
deny     Add a BGP Community List deny rule to Specify community to reject
no       Negate a command or set its defaults
permit   Add a BGP Community List permit rule to Specify community to accept
```

```
clrscr   Clears the display screen
commit   Commit all changes made in this session
do      Run commands from Exec mode
end      End current mode and change to EXEC mode
exit     End current mode and down to previous mode
help     Description of the interactive help system
revert   Revert changes
service  Service Commands
show     Show running system information
write    Write running configuration to memory or terminal
```

```
<DEVICE>(config-bgp-community-list-<COMMUNITY-LIST-NAME>)#
```
The following table summarizes the BGP community list configuration commands:

**Table 28.4  BGP-Community-List-Config Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates and configures a deny community (expanded or standard) rule</td>
<td>page 28-17</td>
</tr>
<tr>
<td>permit</td>
<td>Creates and configures a permit community (expanded or standard) rule</td>
<td>page 28-19</td>
</tr>
<tr>
<td>no</td>
<td>Removes an existing deny or permit community rule from this community list</td>
<td>page 28-21</td>
</tr>
</tbody>
</table>
28.4.1 deny

bgp-community-list-config commands

Creates and configures a deny community (expanded or standard) rule

Standard community lists specify known communities and community numbers. Expanded community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

deny community [expanded|standard]
deny community expanded <LINE>
deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]

Parameters
- deny community expanded <LINE>
- deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]

Examples

nx9500-6C8809(config-bgp-community-list-test)#deny community expanded 100

nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#

nx9500-6C8809(config)#show context
! Configuration of NX9500 version 5.8.1.0-037B
! version 2.3
!

bgp ip-prefix-list PrefixList_01
deny prefix-list 1 192.163.0.0/16 ge 17 le 17
!
bgp ip-prefix-list test
deny prefix-list 1 168.192.13.0/24
permit prefix-list 2 172.122.10.0/24
!
bgp community-list test
deny community expanded 100
!
--More--
nx9500-6C8809(config)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the specified deny community rule from this community list</td>
</tr>
</tbody>
</table>
28.4.2 permit

**bgp-community-list-config commands**

Creates and configures a permit community (expanded or standard) rule

Standard community lists specify known communities and community numbers. Expanded community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit community [expanded|standard]
permit community expanded <LINE>
permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

**Parameters**

- `permit community expanded <LINE>`
  - Configures a permit expanded community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the community attributes.
  - `<LINE>` – Provide the regular expression.

- `permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]`
  - Configures a permit standard community list entry and associates it with a predefined, globally used, known community or community number. The options are:
    - `aa:nn` – Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.
    - `internet` – Advertises this route to the internet community
    - `local-AS` – Prevents transmission of this route outside the local AS
    - `no-advertise` – Prevents advertisement of this route to any peer (internal or external)
    - `no-export` – Prevents advertisement of this route to external BGP peers (keeping this route within an AS)

**Examples**

```
nx9500-6C8809(config-bgp-community-list-test)#permit community expanded 300

nx9500-6C8809(config-bgp-community-list-test)# show context bgp community-list test
  permit community expanded 300
  deny community expanded 100

nx9500-6C8809(config-bgp-community-list-test)#

nx9500-6C8809(config-bgp-community-list-test1)#permit community standard no-export

nx9500-6C8809(config-bgp-community-list-test1)#show context bgp community-list test1
  permit community standard no-export

nx9500-6C8809(config-bgp-community-list-test1)#
```
nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 5.8.1.0-041R
!
! version 2.3
!
! ........................................................
!
! bgp ip-prefix-list PrefixList_01
deny prefix-list 1 192.163.0.0/16 ge 17 le 17 
!
bgp ip-prefix-list test
deny prefix-list 1 168.192.13.0/24
permit prefix-list 2 172.122.10.0/24 
!
bgp community-list test
permit community expanded 300
deny community expanded 100 
!
bgp community-list test1
permit community standard no-export
!
--More--
x9500-6C8809(config)#

**Related Commands**

| *no* | Removes the specified permit community rule from this community list |
28.4.3  no

- **bgp-community-list-config commands**

Removes a deny or permit community rule from this community list

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [deny|permit] community expanded <LINE>

no [deny|permit] community standard [AA:NN|internet|local-AS|no-advertise|no-export]

**Parameters**

- no <PARAMETERS>

  no <PARAMETERS> Removes a deny or permit expanded community rule from this community list
  - <LINE> – Specify the regular expression associated with the rule.

**Examples**

The following example shows the settings of the community list ‘test’ before the ‘no’ command is executed:

nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
  permit community expanded 300
  deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#

nx9500-6C8809(config-bgp-community-list-test)#no deny community expanded 100

The following example shows the settings of the community list ‘test’ after the ‘no’ command is executed:

nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
  permit community expanded 300
nx9500-6C8809(config-bgp-community-list-test)#
28.5 bgp-extcommunity-list-config commands

- **BORDER GATEWAY PROTOCOL**

Creats an configures a named extended community list

A BGP extended community is a group of routes sharing a common attribute, regardless of their network or physical boundary. By using a BGP extended community attribute, routing policies can implement inbound or outbound route filters based on the extended community tag, rather than a long list of individual permit or deny rules. A BGP extended community list is used to create groups of communities to use in a match clause of a route map. An extended community list is used to control which routes are accepted, preferred, distributed, or advertised.

The BGP extended community and standard community attributes are identical in function and structure, except that the former is an eight octet and the latter is a four octet attribute.

BGP extended community lists are used as match clauses in the following context:

- BGP route map context. For more information, see **match**.

To navigate to the extended community configuration instance, use the following command:

```
<DEVICE>(config)#bgp extcommunity-list <EXTCOMMUNITY-LIST-NAME>
```

```
<DEVICE>(config-bgp-extcommunity-list-<EXTCOMMUNITY-LIST-NAME>)#?
```

**BGP Extcommunity List Mode commands**:

- `deny` Add a BGP Community List deny rule to specify extcommunity to reject
- `no` Negate a command or set its defaults
- `permit` Add a BGP Community List permit rule to specify extcommunity to accept
- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
- `end` End current mode and change to EXEC mode
- `exit` End current mode and down to previous mode
- `help` Description of the interactive help system
- `revert` Revert changes
- `service` Service Commands
- `show` Show running system information
- `write` Write running configuration to memory or terminal

```
<DEVICE>(config-bgp-excommunity-list-<EXTCOMMUNITY-LIST-NAME>)#
```

The following table summarizes the BGP extended community list configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates and configures a deny extended community (expanded or standard) rule</td>
<td>page 28-23</td>
</tr>
<tr>
<td>permit</td>
<td>Creates and configures a permit extended community (expanded or standard) rule</td>
<td>page 28-24</td>
</tr>
<tr>
<td>no</td>
<td>Removes an existing deny or permit extended community rule from this extcommunity list</td>
<td>page 28-26</td>
</tr>
</tbody>
</table>
### 28.5.1 deny

**bgp-extcommunity-list-config commands**

Creates and configures a deny extended community (expanded or standard) rule

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

deny extcommunity [expanded|standard]
deny extcommunity expanded <LINE>
deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>

**Parameters**

- **deny extcommunity expanded <LINE>**
  - Configures a deny expanded named extended community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the extended community attributes.
  - `<LINE>` – Provide the regular expression.

- **deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>**
  - Configures a deny standard named extended community list entry and associates it with the target or origin community attributes.
  - **rt** – Configures the route target (RT) extended community attribute
  - **soo** – Configures the site-of-origin (SOO) extended community attribute
  - `<COMMUNITY-NUMBER>` – Specify the community number in one of the following formats: `AA:NN` or `A.B.C.D:NN`

**Examples**

nx9500-6C8809(config-bgp-extcommunity-list-test)#deny extcommunity standard rt 200:12

nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bip extcommunity-list test
deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#

nx9500-6C8809(config)#show context
!
| Configuration of NX9500 version 5.8.1.0-041R
|!
|!
| version 2.3
|!
|---------------------------
| bip community-list test1
|   permit community standard no-export
|!
| bip extcommunity-list test
deny extcommunity standard rt 200:12
|!
|--More--
nx9500-6C8809(config)#

**Related Commands**

- **no**
  - Removes the specified deny extended community rule from this extcommunity list
### 28.5.2 permit

**bgp-extcommunity-list-config commands**

Creates and configures a permit extended community (expanded or standard) rule

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit extcommunity [expanded|standard]
permit extcommunity expanded <LINE>
permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

**Parameters**

<table>
<thead>
<tr>
<th>permit extcommunity expanded &lt;LINE&gt;</th>
<th>Configures a permit expanded named extended community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the extended community attributes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;LINE&gt; – Provide the regular expression.</td>
<td></td>
</tr>
</tbody>
</table>

| permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER> | Configures a permit standard named extended community list entry and associates it with the target or origin community attributes. |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| rt – Configures the RT extended community attribute      |
| soo – Configures the SOO extended community attribute    |
| <COMMUNITY-NUMBER> – Specify the community number in one of the following formats: AA:NN or A.B.C.D:NN |

**Examples**

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#permit extcommunity standard rt 192.168.13.13:12
```

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
  permit extcommunity standard rt 192.168.13.13:12
deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```

```
nx9500-6C8809(config)#show context
  !
  Configuration of NX9500 version 5.8.1.0-041R
  !
  version 2.3
  !
  .....
  !
  bgp community-list test1
  permit community standard no-export
  !
  bgp extcommunity-list test
  permit extcommunity standard rt 192.168.13.13:12
deny extcommunity standard rt 200:12
!--More--
```

```
nx9500-6C8809(config)#
```
<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the specified permit extended community rule from this extcommunity list</td>
</tr>
</tbody>
</table>
28.5.3 no

- **bgp-extcommunity-list-config commands**

Removes an existing deny or permit extended community rule from this extcommunity list.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [deny|permit] extcommunity expanded <LINE>

no [deny|permit] extcommunity standard [rt|soo] <COMMUNITY-NUMBER>

**Parameters**

- no <PARAMETERS>

| no <PARAMETERS> | Removes a deny or permit expanded extended community rule from this community list |

**Examples**

The following example shows the extended community ‘test’ settings before the ‘no’ command is executed:

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
  permit extcommunity standard rt 192.168.13.13:12
  deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#no permit extcommunity standard 192.168.13.13:12
```

The following example shows the extended community ‘test’ settings after the ‘no’ command is executed:

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
  deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```
28.6  bgp-route-map-config commands

BORDER GATEWAY PROTOCOL

BGP route maps are used to control and modify routing information. A BGP route map is a collection of deny and/or permit route rules that define and control redistribution of routes between routers and routing processes. Each rule consists of match criteria and set lines. If a route matches a criteria, the corresponding set line is applied, and the route is passed to the BGP table or to the neighbor, depending on whether the route map is set for incoming or outgoing route updates.

Use the (config) instance to configure BGP route map related parameters.

To navigate to this instance, use the following command:

<DEVICE>(config)#route-map <ROUTE-MAP-NAME>

<DEVICE>(config)#route-map test
<DEVICE>(config-dr-route-map-test)#?

Route Map Mode commands:
- deny Add a deny route map rule to deny set operations
- no Negate a command or set its defaults
- permit Add a permit route map rule to permit set operations
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- exit End current mode and change to EXEC mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal

<DEVICE>(config-dr-route-map-test)#

In the route-map configuration mode, use the following commands to create and configure a deny or permit route map rule:

<DEVICE>(config-dr-route-map-test)#deny route-map <1-65535>
<DEVICE>(config-dr-route-map-test)#permit route-map <1-65535>

For example:

<DEVICE>(config-dr-route-map-test)#permit route-map 1
<DEVICE>(config-dr-route-map-test)#deny route-map 2

<DEVICE>(config-dr-route-map-test)#show context
route-map test
  permit route-map 1
  deny route-map 2
<DEVICE>(config-dr-route-map-test)#

<DEVICE>(config-dr-route-map-test-dr-route-map-rule-1)#?

Route Map Rule Mode commands:
- description Configure comment for this route map
- match Match values from routing table
- no Negate a command or set its defaults
- set Set values in destination routing protocol
- clrscr Clears the display screen
- commit Commit all changes made in this session
- do Run commands from Exec mode
- end End current mode and change to EXEC mode
- exit End current mode and down to previous mode
- help Description of the interactive help system
- revert Revert changes
- service Service Commands
- show Show running system information
- write Write running configuration to memory or terminal
The following table summarizes BGP deny/permit route map rules configuration mode commands:

**Table 28.6 BGP-Route-Map-Config-Mode Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Configures a description for this route-map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions</td>
<td>page 28-29</td>
</tr>
<tr>
<td>match</td>
<td>Configures the match criteria associated with this deny or permit BGP route map</td>
<td>page 28-30</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the settings defined for a deny or permit route-map rule</td>
<td>page 28-33</td>
</tr>
<tr>
<td>set</td>
<td>Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules</td>
<td>page 28-34</td>
</tr>
</tbody>
</table>
28.6.1 **description**

- **bgp-route-map-config commands**

  Configures a description for this route map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions.

  Supported in the following platforms:
  - Wireless Controllers — RFS4000, RFS6000
  - Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

description <LINE>

**Parameters**

- description <LINE>

<table>
<thead>
<tr>
<th>description &lt;LINE&gt;</th>
<th>Provide a description for the route map rule (should not exceed 64 characters in length)</th>
</tr>
</thead>
</table>

**Examples**

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#description "This is a deny route map rule"
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
  description "This is a deny route map rule"
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

**Related Commands**

| no | Removes this deny/permit route-map rule's description |
28.6.2 match

**Bgp-route-map-config commands**

Configures the match criteria associated with this deny or permit BGP route map

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
match [as-path | community | extcommunity | ip-address | ip-next-hop | ip-route-source | metric | origin | tag]
match [as-path <AS-PATH-LIST-NAME> | community <COMMUNITY-LIST-NAME> {exact-match}] | extcommunity <EXTCOMMUNITY-LIST-NAME>]
match [ip-address | ip-next-hop | ip-route-source] [BGP-IP-ACCESS-LIST <BGP-ACL-NAME> | prefix-list <PREFIX-LIST-NAME>]
match metric <0-4294967295>
match origin [egp | igp | incomplete]
match tag <0-65535>
```

**Parameters**

- **match [as-path <AS-PATH-LIST-NAME> | community <COMMUNITY-LIST-NAME> {exact-match}] | extcommunity <EXTCOMMUNITY-LIST-NAME>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| as-path <AS-PATH-LIST-NAME> | Configures a BGP AS path list to match
  An AS path is a list of ASs a packet traverses to reach its destination.
  - <AS-PATH-LIST-NAME> – Specify the AS path list name (should be existing and configured)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| community <COMMUNITY-LIST-NAME> {exact-match} | Configures the AS community list string to match
  - <COMMUNITY-LIST-NAME> – Specify the AS community list name (should be existing and configured).
  - exact-match – Optional. Does an exact match when matching the specified AS community string. This option is disabled by default.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| extcommunity <EXTCOMMUNITY-LIST-NAME> | Configures the external community list string to match
  - <EXTCOMMUNITY-LIST-NAME> – Specify the external community list name (should be existing and configured).

- **match [ip-address | ip-next-hop | ip-route-source] [BGP-IP-ACCESS-LIST <BGP-ACL-NAME> | prefix-list <PREFIX-LIST-NAME>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip-address [BGP-IP-ACCESS-LIST <BGP-ACL-NAME> | prefix-list <PREFIX-LIST-NAME>] | Configures a string of IP addresses, in the route, to match
  The *IP Address* is a list of IP addresses in the route used to filter the route. Use one of the following options to provide a list of IP addresses:
  - BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured).
  - prefix-list <PREFIX-LIST-NAME> – Associates an existing IP address prefix list with this BGP route map. The *IP Address Prefix List* is a list of prefixes in the route used to filter route. Specify the prefix list name (should be existing and configured).
<table>
<thead>
<tr>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-next-hop</strong></td>
<td>Configures the next-hop's IP address to match. The <em>IP Next Hop</em> is a list of IP addresses used to filter routes based on the IP address of the next-hop in the route. Use one of the following options to provide next-hop's IP addresses:</td>
</tr>
<tr>
<td><code>[BGP-IP-ACCESS-LIST &lt;BGP-ACL-NAME&gt;]</code></td>
<td>Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured).</td>
</tr>
<tr>
<td><code>prefix-list &lt;PREFIX-LIST-NAME&gt;]</code></td>
<td>Associates an existing IP next-hop prefix list with this BGP route map. The <em>IP Next Hop Prefix List</em> is a list of prefixes for the route's next-hop determining how the route is filtered. Specify the prefix list name (should be existing and configured).</td>
</tr>
<tr>
<td><strong>ip-route-source</strong></td>
<td>Configures the advertised route source IP address to match. The <em>IP Route Source</em> is a list of IP addresses used to filter routes based on the advertised IP address of the source. Use one of the following options to provide route-source IP addresses:</td>
</tr>
<tr>
<td><code>[BGP-IP-ACCESS-LIST &lt;BGP-ACL-NAME&gt;]</code></td>
<td>Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured).</td>
</tr>
<tr>
<td><code>prefix-list &lt;PREFIX-LIST-NAME&gt;</code></td>
<td>Associates an existing IP route source prefix list with this BGP route map. The <em>IP Route Source Prefix List</em> is a list of prefixes used to filter routes based on the prefix list used for the source. Specify the prefix list name (should be existing and configured).</td>
</tr>
<tr>
<td><strong>match metric &lt;0-4294967295&gt;</strong></td>
<td>Defines the exterior metric, used for route map distribution, to match. BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost.</td>
</tr>
<tr>
<td>**match origin [egp</td>
<td>igp</td>
</tr>
<tr>
<td><code>[egp]</code></td>
<td>Matches if the origin of the route is from the <em>exterior gateway protocol</em> (eBGP). eBGP exchanges routing table information between hosts outside an autonomous system.</td>
</tr>
<tr>
<td><code>[igp]</code></td>
<td>Matches if the origin of the route is from the <em>interior gateway protocol</em> (iBGP). iBGP exchanges routing table information between routers within an autonomous system.</td>
</tr>
<tr>
<td><code>[incomplete]</code></td>
<td>Matches if the origin of the route is not identifiable.</td>
</tr>
<tr>
<td><strong>match tag &lt;0-65535&gt;</strong></td>
<td>Configures the BGP route tag to match. The <em>Tag</em> is a way to preserve a route’s AS path information for routers in iBGP. This option is disabled by default.</td>
</tr>
<tr>
<td><code>&lt;0-65535&gt;</code></td>
<td>Specify the iBGP route’s tag from 0 - 65535.</td>
</tr>
</tbody>
</table>
Examples
The following examples show the configuration of match criteria for the deny route-map rule 1:
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#match as-path FilterList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#match ip-route-source prefix-list PrefixList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
description "This is a deny route map rule"
motion as-path FilterList_01
motion ip-route-source prefix-list PrefixList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#

A permit route-map rule 2 is added to the BGP route-map "test".
nx9500-6C8809(config-dr-route-map-test)#permit route-map 2

A match criteria is added for the permit route-map rule 2.
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#show context
permit route-map 2
motion ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#

The following example displays the BGP route-map “test” settings:
nx9500-6C8809(config-dr-route-map-test)#show context
route-map test
deny route-map 1
description "This is a deny route map rule"
motion as-path FilterList_01
motion ip-route-source prefix-list PrefixList_01
permit route-map 2
motion ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test)#

Related Commands

| no | Removes match criteria associated with a deny or permit route-map rule |
28.6.3 no

- **bgp-route-map-config commands**

Removes or reverts the settings defined for a deny or permit route-map rule

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
no [description|match <PARAMETERS>|set <PARAMETERS>]
```

Parameters

- no <PARAMETERS>

Examples

The following example shows the 'deny route-map rule-1' settings before the 'no' commands are executed:

```plaintext
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
  description "This is a deny route map rule"
  match as-path FilterList_01
  match ip-route-source prefix-list PrefixList_01
  set aggregator-as 1 192.168.13.7
  set as-path exclude 20
  set ip next-hop peer-address
  set metric 300
  set local-preference 30
  set community internet
```

The following example shows the 'deny route-map rule-1' settings after the 'no' commands are executed:

```plaintext
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no match as-path
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no set aggregator-as
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no set metric
```

The following example shows the route-map 'test' settings:

```plaintext
nx9500-6C8809(config-dr-route-map-test)#show context
route-map test
deny route-map 1
  description "This is a deny route map rule"
  match ip-route-source prefix-list PrefixList_01
  set as-path exclude 20
  set ip next-hop peer-address
  set local-preference 30
  set community internet
permit route-map 2
  match ip-next-hop DL_01
```

nx9500-6C8809(config-dr-route-map-test)#
28.6.4 set

**bgp-route-map-config commands**

Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules. These attributes are applied before the route is sent out.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
set [aggregator-as|as-path|atomic-aggregate|comm-list|community|extcommunity|ip|
  local-preference|metric|origin|originator-id|source-ip|tag|weight]
```

```
set aggregator-as <1-4294967295> <IP>
set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}
set atomic-aggregate
set comm-list delete <COMMUNITY-LIST-NAME>
set community [<COMMUNITY-NUMBER>|none]
set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>
set ip next-hop [<IP>|peer-address]
set local-preference <0-4294967295>
set metric <0-4294967295>
set origin [egp|igp|incomplete]
set originatorid <IP>
set source-ip <IP>
set tag <0-65535>
set weight <0-4294967295>
```

**Parameters**
- set aggregator-as <1-4294967295> <IP>

<table>
<thead>
<tr>
<th>set aggregator-as &lt;1-4294967295&gt; &lt;IP&gt;</th>
<th>Configures the BGP aggregator’s ASN and IP address. Aggregates minimize the size of routing tables. Aggregation combines the characteristics of multiple routes and advertises them as a single route. The configured BGP aggregator settings are applied to filtered routes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;1-4294967295&gt; – Specify the route aggregator’s ASN from 1- 4294967295. This option is disabled by default.</td>
<td></td>
</tr>
<tr>
<td>• &lt;IP&gt; – Specify the route aggregator’s IP address. BGP allows the aggregation of specific routes into one route using an aggregate IP address.</td>
<td></td>
</tr>
</tbody>
</table>
### set as-path [exclude|prepend] <1-4294967295> \(\{<1-4294967295>\}\)

Configures the BGP transform AS path attribute to be applied to filtered routes
- exclude – Configures a single AS, or a list of ASs, excluded from the AS path
- prepend – Configures a single AS, or a list of ASs, prepended to the AS path

- `<1-4294967295>` – This keyword is common to the ‘exclude’ and ‘prepend’ parameters. Use it to specify the AS number. The ASs identified here are excluded or prepended depending on the option selected.

**Note:** You can configure multiple ASNs.

### set atomic-aggregate

**set atomic-aggregate**

Enables BGP atomic aggregate attributes

When a BGP enabled wireless controller or service platform receives a set of overlapping routes from a peer, or if the set of routes selects a less specific route, then the local device must set this value when propagating the route to its neighbors. This option is disabled by default.

### set comm-list delete <COMMUNITY-LIST-NAME>

**set comm-list delete <COMMUNITY-LIST-NAME>**

Deletes specified BGP communities. All communities matching the community list name string are deleted from the route.

A BGP community is a group of routes sharing a common attribute.
- `<COMMUNITY-LIST-NAME>` – Specify the community list name.

### set community [<COMMUNITY-NUMBER>|none]

**set community [<COMMUNITY-NUMBER>|none]**

Configures a community attribute for this route
- `<COMMUNITY-NUMBER>` – Specify a community attribute. Use one of the following formats:
  - internet - Advertises this route to the Internet. This is a global community.
  - local-AS - Prevents the transit of packets outside the local AS
  - no-advertise - Prevents advertisement of this route to any peer, either internal or external
  - no-export - Prevents advertisement of this route to BGP peers, keeping this route within an AS.
  - aa:nn - Configures the first part (aa) representing the AS number. The second part (nn) represents a 2-byte number.
- none – Specifies community attribute as none

### set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>

**set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>**

Configures a extended community attribute for this route
- rt – Identifies the route target (rt) extended community
- soo – Identifies the site-of-origin (soo) community. This is the origin community associated with the route reflector.
- `<EXTCOMMUNITY-NUMBER>` – This keyword is common to the ‘rt’ and ‘soo’ parameters. Use it to specify the extended community number.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| set ip next-hop [IP|peer-address]                  | Configures the next hop for this route. Use one of the following options to identify the next hop:  
|                               | • IP – Specify the next hop’s IP address  
|                               | • peer-address – Enables the identification of the next-hop address for peer devices. This option is disabled by default |
| set local-preference 0-4294967295 | Configures the BGP local preference path attribute for this route map. When configured, enables the communication of preferred routes out of the AS between peers. This option is disabled by default  
|                               | • 0-4294967295 – Specify the preference value from 0 - 4294967295.                                                                                   |
| set metric 0-4294967295       | Configures a metric for the route  
|                               | BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost.  
|                               | • 0-4294967295 – Specify the metric from 0 - 4294967295.                                                                                      |
| set origin [egp|igp|incomplete] | Configures the origin code for this BGP route map  
|                               | • egp - Sets the origin of the route to eBGP  
|                               | • igp - Sets the origin of the route to iBGP  
|                               | • incomplete - Sets the origin of the route as not identifiable. Use this option if the route is from a source other than eBGP or iBGP.       |
| set originorid IP             | Configures this route map’s originator IP address                                                                                             |
| set source-ip IP              | Configures this route map’s source IP address  
|                               | • IP – Specify the IP address in the A.B.C.D format.                                                                                             |
| set tag 0-65535               | Configures this route map’s tag value  
|                               | The Tag is a way to preserve a route’s AS path information for routers in iBGP.  
|                               | • 0-65535 – Specify a tag value from 0 - 65535.                                                                                           |
| set weight 0-4294967295       | Enables assignment of a weighted priority to the aggregate route  
|                               | • 0-4294967295 – Specify a value from 0 - 4294967295.                                                                                  |
Examples

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set aggregator-as 1 192.168.13.7

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set as-path exclude 20

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set community internet

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set ip next-hop peer-address

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set local-preference 30

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set metric 300

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context deny route-map 1
description "This is a deny route map rule"
match as-path FilterList_01
match ip-route-source prefix-list PrefixList_01
set aggregator-as 1 192.168.13.7
set as-path exclude 20
set ip next-hop peer-address
set metric 300
set local-preference 30
set community internet

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the attributes configured for this route map</td>
</tr>
</tbody>
</table>
28.7 bgp-router-config commands

Use the (device-config) or (profile-config) instance to configure BGP router related parameters.

To navigate to the BGP router configuration instance, in the device-config mode, use the following commands:

<DEVICE>(config)#self
<DEVICE>(config-device-<MAC>)#router bgp
<DEVICE>config-device <MAC>-router-bgp)#

<DEVICE>config-device <MAC>-router-bgp)#?

When configured as a profile, the router settings are applied to all devices using the profile.

To navigate to the BGP router configuration instance, in the profile-config mode, use the following commands:

<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#router bgp
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#

<DEVICE>config-device <MAC>-router-bgp)#

Router BGP Mode commands:

- aggregate-address: Configure aggregate address
- asn: Configure local Autonomous System Number
- bgp: Border Gateway Protocol
- bgp-route-limit: Limit for number of routes handled by BGP process
- distance: Configure administrative distance
- ip: Internet Protocol (IP)
- network: Configure a local network
- no: Negate a command or set its defaults
- route-redistribute: Redistribute information from another routing protocol
- timers: Adjust routing timers
- clrscr: Clears the display screen
- commit: Commit all changes made in this session
- do: Run commands from Exec mode
- end: End current mode and change to EXEC mode
- exit: End current mode and down to previous mode
- help: Description of the interactive help system
- revert: Revert changes
- show: Show running system information
- write: Write running configuration to memory or terminal
The following table summarizes BGP router configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate-address</td>
<td>Creates and configures an aggregate address entry in the BGP database</td>
<td>page 28-40</td>
</tr>
<tr>
<td>asn</td>
<td>Configures this BGP router’s ASN</td>
<td>page 28-41</td>
</tr>
<tr>
<td>bgp</td>
<td>Configures BGP router parameters</td>
<td>page 28-42</td>
</tr>
<tr>
<td>bgp-route-limit</td>
<td>Configures the BGP route limit parameters</td>
<td>page 28-46</td>
</tr>
<tr>
<td>distance</td>
<td>Configures administrative distance parameters</td>
<td>page 28-47</td>
</tr>
<tr>
<td>ip</td>
<td>Configures the BGP default gateway’s priority</td>
<td>page 28-48</td>
</tr>
<tr>
<td>network</td>
<td>Configures the local network IP addresses and masks</td>
<td>page 28-49</td>
</tr>
<tr>
<td>no</td>
<td>Removes the BGP router settings</td>
<td>page 28-50</td>
</tr>
<tr>
<td>route-redistribute</td>
<td>Enables redistribution of routes learnt from other routing protocols into BGP</td>
<td>page 28-51</td>
</tr>
<tr>
<td>timers</td>
<td>Enables adjustment of keepalive and holdtime intervals</td>
<td>page 28-53</td>
</tr>
</tbody>
</table>
28.7.1 aggregate-address

btc-router-config commands

Creates and configures an aggregate address entry in the BGP database

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
aggregate-address <IP/M> {as-set {summary-only}|summary-only}

Parameters
- aggregate-address <IP/M> {as-set {summary-only}|summary-only}

Examples
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#aggregate-address
192.168.13.10/32 as-set summary-only

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
bgp enable
asn 1
aggregate-address 192.168.13.10/32 as-set summary-only
bgp neighbor 192.168.13.199
remote-as 1
use route-map UnSupMap_01 in
bgp neighbor 192.168.13.99
remote-as 199
timers connect 10
timers 20 40
maximum-prefix 9999 80 restart 50
bgp neighbor 1.1.1.1
remote-as 2
timers connect 10
timers 20 40
maximum-prefix 1000000
bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

Related Commands

no Removes the aggregate address entry
28.7.2 *asn*

- **bgp-router-config commands**

Configures the ASN. The ASN represents a group of routers under the same administration and using IGP and common metrics to define how to route packets. In short the ASN represents all routers within an AS.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`asn <1-4294967295>`

**Parameters**

- `asn <1-4294967295>`

---

**Examples**

```
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#asn 1
```

```
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#show context router bgp
  asn 1
```

```
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#
```
## 28.7.3 bgp

### bgp-router-config commands

Configures BGP router parameters

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

### Syntax

```
bgp [always-compare-med|bestpath|client-to-client|cluster-id|confederation|dampening|default|deterministic-med|enable|enforce-first-as|fast-external-failover|graceful-restart|log-neighbor-changes|neighbor|network|router-id|scan-time]

bgp [always-compare-med|deterministic-med|enable|enforce-first-as|fast-external-failover|log-neighbor-changes]

bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-worst}|missing-as-worst}]

bgp cluster <IP>

bgp confederation [identifier|peers] <1-4294967295>

bgp dampening [<1-45>] [<1-20000>] <1-255>

bgp default [ipv4-unicast|local-preference <0-4294967295>]

bgp graceful-restart {stalepath-time <1-3600>}

bgp neighbor <IP>

bgp network import-check

bgp router-id <IP>

bgp scan-time <5-60>
```

### Parameters

- **always-compare-med**: Enables comparison of Multi-exit Discriminators (MEDs) received from neighbors. This option is disabled by default.
  
  MED is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared when selecting the best route to the host network. A route with a lower MED value is preferred over a route with a higher MED value. BGP does not discriminate between iBGP and eBGP when using MED for route selection. This option is mutually exclusive to the `deterministic-med` option.

- **deterministic-med**: Enables selection of the best MED path from amongst all paths advertised by neighboring ASs. This option is disabled by default.
  
  MED is used by BGP peers to select the best route among multiple routes. When enabled, MED route values (from the same AS) are compared to select the best route. This best route is then compared with other routes in the BGP route table to select the best overall route. This option is mutually exclusive to the `always-compare-med` option.

- **enable**: Starts the BGP daemon on the device (wireless controller or service platform). BGP is disabled by default.

- **enforce-first-as**: Enforces the first AS for all BGP routes. This option is disabled by default.
  
  When enforced, devices deny updates received from an external neighbor that does not have the neighbor’s configured AS at the beginning of the received AS path parameter. This enhances security by not allowing traffic from an unauthorized AS.
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast-external-failover</td>
<td>Enables immediate resetting of BGP session on the interface once the BGP connection goes down. This option is enabled by default. When enabled, a session is reset as soon as the direct link to an external peer goes down. Normally, when a BGP connection goes down, the device waits for the expiry of the duration specified in <code>holdtime</code> parameter before bringing down the interface. <strong>Note:</strong> To configure the 'holdtime', use the <code>timers &gt; bgp &gt; &lt;keepalive-time&gt; &gt; &lt;holdtime&gt;</code> command in this (BGP router) configuration mode.</td>
</tr>
<tr>
<td>log-neighbor-changes</td>
<td>Enables logging of a BGP neighbor’s status change (active or not active) events. It also enables the logging of the reason for such change in status.</td>
</tr>
</tbody>
</table>

- `bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-worst}|missing-as-worst}]`

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-path</td>
<td>Modifies the bestpath selection algorithm. The route selection algorithm uses the following criteria when selecting the preferred route: as-path, router-id, and med.</td>
</tr>
</tbody>
</table>
| as-path [confed|ignore] | Enables an AS path from being considered as a criteria for selecting the preferred route  
  - confed – Enables comparison of path lengths (including confederation sets and sequences) when selecting a route (EXPERIMENTAL). This option is disabled by default.  
  - ignores – Disables an AS path length from being considered as a criteria for selecting a preferred route. When, disabled the AS path length is ignored. This option is disabled by default. |
| compare-router-id     | Enables the use of router ID as a selection criteria when selecting the preferred route. When enabled, the router ID is used to select the best path between two identical BGP routes. The route with the lower router ID is selected over a route with a higher router ID. This option is disabled by default. |
| med {confed {missing-as-worst}|missing-as-worst} | Enables comparison of AS path MED value when selecting the preferred route  
  MED is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared to determine the best route to the host network. A route with a lower MED value is preferred over a route with a higher MED value.  
  - confed – Optional. Enables comparison of MED value among confederation paths (EXPERIMENTAL). When enabled, you can optionally enable the treatment of AS paths without the MED value as the least preferable route. This option is disabled by default.  
  - missing-as-worst – Optional. Enables the treatment of AS paths without the MED value as the least preferable route. This option is disabled by default. |

- `bgp client-to-client reflection`

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| client-to-client reflection | Enables client-to-client route reflection (EXPERIMENTAL)  
Route reflectors are used when all iBGP speakers are not fully meshed. If the clients are fully meshed, the route-reflectors are not required. This option is enabled by default. |

- `bgp cluster <IP>`

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| cluster <IP>           | Enables and sets a cluster ID, in case the BGP cluster has more than one route-reflector  
A cluster generally consists of a single route-reflector and its clients. The cluster is usually identified by the router ID of this single route-reflector. Sometimes, to increase redundancy, a cluster might have more than one route-reflector configured. In this case, all route-reflectors in the cluster are identified by the cluster ID (configured in the IP format). |
- **bgp confederation [identifier|peers] <1-4294967295>**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| confederation [identifier|peers] <1-4294967295> | Configures AS confederation (group of ASs) parameters (identifier and peers)
  - identifier – Enables and sets a BGP confederation identifier to allow an AS to be divided into several ASs. In other words an AS is divided into multiple ASs, and together they form a confederation. This confederation is visible to external routers as a single AS. The ASN is usually the confederation ID. Specify a value from 1 - 4294967295.
  - peers – Configures the maximum number of the ASs constituting this BGP confederation. Specify the AS number from 1 - 4294967295. Multiple ASs can be added to the list of confederation members. |

- **bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255>**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255> | Enables dampening and configures dampening parameters. This option is disabled by default.
  - Dampening minimizes the instability caused by route flapping. A penalty is added for every flap in the flapping route. As soon as the total penalty reaches the specified Route Suppress Limit value, the advertisement of this route is suppressed. This penalty is delayed when the time specified in Half Lifetime occurs. Once the penalty becomes lower than the value specified in Start Route Reuse, the advertisement of the route is unsuppressed.
  - <1-45> – Optional. Configures the half lifetime (in minutes). A penalty is imposed on a route that flaps. This is the time for the penalty to decrease to half its current value. Specify a value from 1 - 45 minutes. The default is 1 minute.
  - <1-20000> – Optional. Configures the route reuse value. When the penalty for a suppressed route decays below the value specified here, the route is unsuppressed (reused). Specify a value from 1 - 20000.
  - <1-20000> – Configures the route suppress value. When a route flaps, a penalty is added to the route. When the penalty reaches or exceeds the value specified as the ‘maximum duration to suppress a stable route’. Specify a value from 1 - 20000.
  - <1-255> – Configures the maximum duration, in minutes, a suppressed route is suppressed. This is the maximum duration for which a route remains suppressed before it is reused. Specify a value from 1 - 255 minutes. |

- **bgp default [ipv4-unicast|local-preference <0-4294967295>]**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures the following defaults for BGP neighbor-related parameters: IPv4 unicast and local preference</td>
</tr>
<tr>
<td>ipv4-unicast</td>
<td>Enable IPv4 unicast traffic for neighbors. This option is enabled by default.</td>
</tr>
</tbody>
</table>
| local-preference <0-4294967295> | Configures a local preference for the neighbor. Higher the value higher is the preference.
  - <0-4294967295> – Specify a value from 0 - 4294967295. |
### BGP Graceful-Restart

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp graceful-restart {stalepath-time &lt;1-3600&gt;}</td>
<td>Enables graceful restart on this BGP router. This option is disabled by default.</td>
</tr>
<tr>
<td><strong>default graceful-restart {stalepath-time &lt;1-3600&gt;}</strong></td>
<td>Enables graceful restart on this BGP router. This option is disabled by default.</td>
</tr>
<tr>
<td><strong>stalepath-time &lt;1-3600&gt;</strong></td>
<td>- Optional. Configures the maximum time, in seconds, to retain stale paths from restarting neighbor. This is the time the paths from a restarting neighbor are preserved. All stale paths, unless reinstated by the neighbor after re-establishment, are deleted at the expiry of the time specified here.</td>
</tr>
<tr>
<td><strong>&lt;1-3600&gt;</strong></td>
<td>- Specify a value from 1 - 3600 seconds.</td>
</tr>
</tbody>
</table>

### BGP Neighbor Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp neighbor &lt;IP&gt;</td>
<td>Configures the BGP neighbor’s IP address and enters its configuration mode. Use this command to configure a BGP neighbor’s parameters.</td>
</tr>
<tr>
<td><strong>neighbor &lt;IP&gt;</strong></td>
<td>Configures the BGP neighbor’s IP address and enters its configuration mode. Use this command to configure a BGP neighbor’s parameters.</td>
</tr>
<tr>
<td><strong>&lt;IP&gt;</strong></td>
<td>- Specify the IP address in the A.B.C.D format.</td>
</tr>
</tbody>
</table>

**Note:** For BGP neighbor configuration parameters, see `bgp-neighbor-config commands`.  

### BGP Network Import Check

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network import-check</td>
<td>Enables checking of the existence of BGP network route in IGP before importing</td>
</tr>
</tbody>
</table>

### BGP Router ID

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp router-id &lt;IP&gt;</td>
<td>Enables the device (BGP supported wireless controller or service platform) identified by the &lt;IP&gt; parameter as a router. The router’s IP address is configured as its ID, and uniquely identifies it. When not specified, the IP address of the interface is configured as the router ID. This option is disabled by default.</td>
</tr>
</tbody>
</table>

### BGP Scan Time

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scan-time &lt;5-60&gt;</td>
<td>Configures the scanning interval, in seconds, for updating BGP routes. This is the interval between two consecutive scans the BGP device performs in order to validate routes in its routing table. To disable scanning, set the value to Zero (0).</td>
</tr>
<tr>
<td><strong>&lt;5-60&gt;</strong></td>
<td>- Specify a value from 5 - 60 seconds. The default is 60 seconds.</td>
</tr>
</tbody>
</table>

### Examples

```
x9500-6C8809(config-profile NX45XXProfile-router-bgp)#bgp router-id 192.168.13.13
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#aggregate-address 116.117.118.0/24 as-set summary-only
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#bgp neighbor 192.168.13.99
```

```
x9500-6C8809(config-profile NX45XXProfile-router-bgp)#show context
          router bgp
            aggregate-address 116.117.118.0/24 as-set summary-only
            bgp router-id 192.168.13.13
            bgp neighbor 192.168.13.99
            remote-as 199
            maximum-prefix 9999 80 restart 50
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the BGP router parameters. The <code>no &gt; bgp &gt; enable</code> command disabled BGP.</td>
</tr>
</tbody>
</table>
28.7.4 bgp-route-limit

Configures the BGP route limit parameters

Supported in the following platforms:
• Wireless Controllers — RFS4000, RFS6000
• Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

bgp-route-limit [num-routes <VALUE>|reset-time <1-86400>|retry-count <1-32>|retry-timeout <1-3600>]

Parameters
• bgp-route-limit [num-routes <VALUE>|reset-time <1-86400>|retry-count <1-32>|retry-timeout <1-3600>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| num-routes <VALUE> | Configures the number of routes that can be stored on this BGP router. Set this value based on the available memory on this BGP router (wireless controller or service platform).  
  • <VALUE> – Specify a value from 1 - 4,294,967,295. The default is 9216 routes. |
| reset-time <1-86400> | Configures the reset time in seconds. This is the time after which the retry count value is set to Zero (0).
  • <1-86400> – Specify a value from 1- 86,400 seconds. The default is 360 seconds. |
| retry-count <1-32> | Configures the maximum number of times the BGP process is reset before being permanently shut down. Once shut down, the BGP process has to be started manually. The BGP process is reset if it is flooded with route entries that exceed the maximum number of routes configured for this device.
  • <1-32> – Specify a value from 1 - 32. The default is 5 routes. |
| retry-timeout <1-3600> | Configures the duration, in seconds, the BGP process is temporarily shut down, before a reset of the process is attempted.
  • <1-3600> – Specify a value from 1 - 3600 seconds. The default is 60 seconds. |

Examples

nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#bgp-route-limit num-routes 10

nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#show context
  router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.99
  remote-as 199
  maximum-prefix 9999 80 restart 50
  bgp-route-limit num-routes 10
  nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#

Related Commands

no

Removes BGP route limitations configured. Use the no command to revert back to default.
**28.7.5 distance**

- **bgp-router-config commands**

Configures administrative distance parameters. The distance parameter is a rating of the trustworthiness of a route. The higher the distance, lower is the trust rating. The distance can be set for each type of route indicating its trust rating.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

distance [IP/M <1-255> <BGP-ACL-NAME>|bgp <1-255> <1-255> <1-255>]

**Parameters**

- distance [IP/M <1-255> <BGP-ACL-NAME>|bgp <1-255> <1-255> <1-255>]

**Examples**

```
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#distance bgp 200 100 200
```

```
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#show context
router bgp
ggp enable
asn 1
aggregate-address 116.117.118.0/24 as-set summary-only
distance bgp 200 100 200
ggp neighbor 192.168.13.99
remote-as 199
maximum-prefix 9999 80 restart 50
ggp-route-limit num-routes 10
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#
```

**Related Commands**

- **no**

  Removes the administrative distance related configurations
28.7.6  ip

*bgp-router-config commands*

Configures the BGP default gateway's priority

Supported in the following platforms:

-  Wireless Controllers — RFS4000, RFS6000
-  Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ip default-gateway priority <1-8000>`

**Parameters**

- `ip default-gateway priority <1-8000>`

| default-gateway priority <1-8000> | Configures the default gateway’s (acquired through BGP) priority  
|-----------------------------------|------------------------------------------------------------------|
| <1-8000>                         | - Specify a value from 1 - 8000. The default is 7500.  
| **Note:** Lower the value, higher is the priority. | |

**Examples**

```
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#ip default-gateway priority 1

nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#show context
    router bgp
        bgp enable
        asn 1
    ip default-gateway priority 1
        bgp-route-limit num-routes 10

nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#
```

**Related Commands**

| no | Removes the BGP default gateway configuration |
28.7.7 \textit{network} \hfill \scriptsize{b}gp-router-config commands

Configures the local network IP addresses and masks. These network addresses are broadcasted to neighboring BGP peers. You can configure a single IP address or a range of IP addresses in the A.B.C.D/M notation.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

\textbf{Syntax}

\begin{verbatim}
network <IP/M> \{\textit{backdoor} | \textit{pathlimit} | \textit{route-map}\}
network <IP/M> \{\textit{backdoor} \textit{pathlimit} <1-255>\}
network <IP/M> \{\textit{pathlimit} <1-255>\}
network <IP/M> \{\textit{route-map} \textit{<ROUTE-MAP-NAME>}\}
\end{verbatim}

\textbf{Parameters}

- \texttt{network <IP/M> \{\textit{backdoor} \textit{pathlimit} <1-255>\} | \textit{pathlimit} <1-255>\} | \textit{route-map} \textit{<ROUTE-MAP-NAME>}}\}

| network <IP/M> | Configures the local network's address in the A.B.C.D/M format
| \begin{itemize}
| \item <IP/M> – Specify the network address.
\end{itemize} |

| backdoor pathlimit <1-255> | Optional. Configures a BGP backdoor route. After configuring the backdoor route, you can optionally configure the as-path hop count limit attribute for this backdoor route.
| \begin{itemize}
| \item pathlimit <1-255> – Specify the hop count limit from 1 - 255.
\end{itemize} |

| pathlimit <1-255> | Optional. Configures the maximum path limit for this AS
| \begin{itemize}
| \item <1-255> – Specify the hop count limit from 1 - 255.
\end{itemize} |

| route-map <ROUTE-MAP-NAME> | Optional. Associates a BGP route map with this local network. When applied, the route-map values take precedence
| \begin{itemize}
| \item <ROUTE-MAP-NAME> – Specify the route map name.
\end{itemize} |

\textbf{Examples}

\begin{verbatim}
nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#network 192.168.13.0/24 backdoor pathlimit 200

nx9500-6C8809(config-profile NX45XXProfile-router-bgp)#show context router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
distance bgp 200 100 200
bgp neighbor 192.168.13.99
remote-as 199
maximum-prefix 9999 80 restart 50
network 1.2.3.0/24
network 192.168.13.0/24 backdoor pathlimit 200
bgp-route-limit num-routes 10
\end{verbatim}

\textbf{Related Commands}

\texttt{no} | Removes the list of local networks configured
28.7.8 no

**bgp-router-config commands**

Removes the BGP router settings

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [aggregate-address|bgp|bgp-route-limit|distance|ip|network|route-redistribute|timers]

**Parameters**

- no <PARAMETERS>

**Examples**

The following example shows the BGP router settings before the 'no' commands have been executed:

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.199
    remote-as 1
    use route-map UnSupMap_01 in
  bgp neighbor 192.168.13.99
    remote-as 199
    maximum-prefix 9999 80 restart 50
  bgp-route-limit num-routes 10 reset-time 360
```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no bgp neighbor 192.168.13.99
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no aggregate-address 116.117.118.0/24
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no bgp-route-limit
```

The following example shows the BGP router settings after the 'no' commands have been executed:

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
  bgp enable
  asn 1
  bgp neighbor 192.168.13.199
    remote-as 1
    use route-map UnSupMap_01 in
```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#
**28.7.9 route-redistribute**

- **bgp-router-config commands**

Enables redistribution of routes learnt from other routing protocols into BGP.

Large ISP networks using multiple routing protocols need to enable redistribution of routes across routing protocols. Routing protocols differ in their basic characteristics, such as metrics, administrative distance, classful and classless capabilities, etc. When enabling redistribution, these differences have to be taken into consideration.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
route-redistribute [connected|kernel|ospf|static] {metric <0-4294967295>|
route-map <ROUTE-MAP-NAME>}
```

**Parameters**

- route-redistribute [connected|kernel|ospf|static] {metric <0-4294967295>|
route-map <ROUTE-MAP-NAME>}

<table>
<thead>
<tr>
<th>route-redistribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| **connected**      | Redistributes routes learnt from other protocols.  
| route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see [match](#). |
| **kernel**         | Redistributes kernel routes. These are routes that are neither connected, nor static, nor dynamic.  
| route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see [match](#). |
| **ospf**           | Redistributes OSPF routes  
| route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see [match](#). |
| **static**         | Redistributes static routes  
| route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see [match](#). |
Examples

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#route-redistribute connected metric 200

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.99
    remote-as 199
    maximum-prefix 9999 80 restart 50
  bgp neighbor 192.168.13.199
    remote-as 1
    use route-map UnSupMap_01 in
  route-redistribute connected metric 200
  bgp-route-limit num-routes 10 reset-time 360

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables redistribution of routes learnt from other routing protocols into BGP</td>
</tr>
</tbody>
</table>
28.7.10 timers

▶ bgp-router-config commands

Enables adjustment of keepalive and holdtime intervals

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

timers bgp <0-65535> <0-65535>

Parameters

- timers bgp <0-65535> <0-65535>

<table>
<thead>
<tr>
<th>timers bgp &lt;0-65535&gt; &lt;0-65535&gt;</th>
<th>Configures the keepalive and holdtime interval in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;0-65535&gt; – Specify a keepalive interval from 0 - 65535 seconds. It is the interval, in seconds, between two successive keepalive packets exchanged with this router and its neighbor to keep the TCP connection alive.</td>
<td></td>
</tr>
<tr>
<td>• &lt;0-65535&gt; – Specify a holdtime value from 0 - 65535 seconds. This is the time this router will wait without receiving a keepalive packet from its neighbor before declaring it dead. If the time since the last keepalive packet received (from its neighbor) exceeds the value set here, the neighbor is declared dead.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#timers bgp 100 100

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.199
  remote-as 1
  use route-map UnSupMap_01 in
  bgp neighbor 192.168.13.99
  remote-as 199
  maximum-prefix 9999 80 restart 50
  timers bgp 100 100
  bgp-route-limit num-routes 10 reset-time 360

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

Related Commands

- no Reverts BGP timers to default
28.8 bgp-neighbor-config commands

**BORDER GATEWAY PROTOCOL**

BGP enabled devices connected through an established TCP connection are referred to as BGP peers or neighbors. To establish a TCP connection, BGP routers exchange open messages containing the following information: AS number, BGP version running, BGP router ID, and timer values (keepalive and holdtime). Once these values are accepted by both devices, the connection is established and the routers become neighbors. With the TCP connection established the BGP neighbors begin sharing routing information and updates. A failure in the establishment of the TCP connection indicates that the routers are not neighbors and cannot exchange routing information.

Use the (profile/device-config) instance to configure BGP neighbors.

To navigate to the BGP neighbor configuration instance, use the following commands:

```
<DEVICE>(config)#profile <PROFILE-NAME>
<DEVICE>(config-profile <PROFILE-NAME>)#router bgp
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#?
```

```
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#bgp neighbor ?
A.B.C.D  IP address of the bgp neighbor
```

```
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#bgp neighbor <IP>
<DEVICE>(config-profile <PROFILE-NAME>-router--bgp-neighbor-<IP>)#?
```

Router BGP Neighbor Mode commands:

- **activate** Enable the Address Family for this Neighbor (EXPERIMENTAL)
- **advertisement-interval** Minimum interval between BGP routing updates
- **allow-as-in** Accept as-path with my AS present in it (EXPERIMENTAL)
- **attribute-unchanged** BGP attribute is propagated unchanged to this neighbor (EXPERIMENTAL)
- **capability** Advertise capability to the peer
- **default-originate** Originate default route to this neighbor
- **description** Neighbor specific description
- **disable-connected-check** One-hop away EBGP peer using loopback address (EXPERIMENTAL)
- **dont-capability-negotiate** Do not perform capability negotiation (EXPERIMENTAL)
- **ebgp-multihop** Allow EBGP neighbors not on directly connected networks
- **enforce-multihop** Enforce EBGP neighbors perform multihop (EXPERIMENTAL)
- **local-as** Specify a local-as number (EXPERIMENTAL)
- **maximum-prefix** Maximum number of prefix accept from this peer
- **next-hop-self** Disable the next hop calculation for this neighbor
- **no** Negate a command or set its defaults
- **override-capability** Override capability negotiation result
- **passive** Don't send open messages to this neighbor
- **password** Set a password
- **peer-group** Set peer-group for this neighbor (EXPERIMENTAL)
- **port** Neighbor's BGP port (EXPERIMENTAL)
- **remote-as** Specify a BGP neighbor
- **remove-private-as** Remove private AS number from outbound updates (EXPERIMENTAL)
- **route-server-client** Configure a neighbor as Route Server client (EXPERIMENTAL)
- **send-community** Send Community attribute to this neighbor
- **shutdown** Administratively shut down this neighbor
- **soft-reconfiguration** Per neighbor soft reconfiguration
- **strict-capability-match** Strict capability negotiation match (EXPERIMENTAL)
- **timers** BGP per neighbor timers
unsuppress-map          Route-map to selectively unsuppress suppressed routes
update-source           Source of routing updates
use                     Set setting to use
weight                  Set default weight for routes from this neighbor
clrscr                  Clears the display screen
commit                  Commit all changes made in this session
do                      Run commands from Exec mode
end                     End current mode and change to EXEC mode
exit                    End current mode and down to previous mode
help                    Description of the interactive help system
revert                  Revert changes
service                 Service Commands
show                    Show running system information
write                   Write running configuration to memory or terminal

<DEVICE>(config-profile <PROFILE-NAME>-router--bgp-neighbor-<IP>)#

The following table summarizes BGP deny/permit route map rules configuration mode commands:

### Table 28.8 BGP-Neighbor-Config-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>activate</td>
<td>Enables an address family for this neighbor (EXPERIMENTAL)</td>
<td>page 28-57</td>
</tr>
<tr>
<td>advertisement-interval</td>
<td>Configures the minimum interval between two consecutive BGP router updates</td>
<td>page 28-58</td>
</tr>
<tr>
<td>allowas-in</td>
<td>Enables re-advertisement of all prefixes containing duplicate ASNs</td>
<td>page 28-59</td>
</tr>
<tr>
<td>attribute-unchanged</td>
<td>Enables the propagation of BGP attribute values unchanged to this neighbor</td>
<td>page 28-60</td>
</tr>
<tr>
<td>capability</td>
<td>Enables the advertisement of capability (dynamic and ORF) to BGP peers</td>
<td>page 28-61</td>
</tr>
<tr>
<td>default-originate</td>
<td>Enables the sending of the default route to BGP neighbors. It also allows</td>
<td>page 28-62</td>
</tr>
<tr>
<td></td>
<td>the configuration of the default route.</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>Configures a description for a BGP neighbor device</td>
<td>page 28-63</td>
</tr>
<tr>
<td>disable-connected-check</td>
<td>Enables one-hop away EBGP peer using loop back address (EXPERIMENTAL)</td>
<td>page 28-64</td>
</tr>
<tr>
<td>dont-capability-negotiate</td>
<td>Disables capability negotiation with BGP neighbors (EXPERIMENTAL)</td>
<td>page 28-65</td>
</tr>
<tr>
<td>ebgp-multihop</td>
<td>Enables eBGP Multihop on this BGP neighbor, and configures the maximum</td>
<td>page 28-66</td>
</tr>
<tr>
<td></td>
<td>number of hops that can be between eBGP neighbors not directly connected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to each other.</td>
<td></td>
</tr>
<tr>
<td>enforce-multihop</td>
<td>Forces EBGP neighbors to perform multi-hop checks (EXPERIMENTAL)</td>
<td>page 28-67</td>
</tr>
<tr>
<td>local-as</td>
<td>Configures this neighbor’s local AS number. Also enables the prepending of</td>
<td>page 28-68</td>
</tr>
<tr>
<td></td>
<td>this AS number in route updates. (EXPERIMENTAL)</td>
<td></td>
</tr>
<tr>
<td>maximum-prefix</td>
<td>Configures the maximum number of prefixes that can be received from a</td>
<td>page 28-69</td>
</tr>
<tr>
<td></td>
<td>BGP neighbor</td>
<td></td>
</tr>
<tr>
<td>next-hop-self</td>
<td>Enables next-hop calculation for this neighbor</td>
<td>page 28-70</td>
</tr>
<tr>
<td>no</td>
<td>Removes this BGP neighbor’s settings, or reverts them back to default</td>
<td>page 28-71</td>
</tr>
<tr>
<td>override-capability</td>
<td>Enables the overriding of capability negotiation results</td>
<td>page 28-72</td>
</tr>
</tbody>
</table>
### Table 28.8 BGP-Neighbor-Config-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive</td>
<td>Enables this BGP neighbor device (or devices using this profile) as passive</td>
<td>page 28-73</td>
</tr>
<tr>
<td>password</td>
<td>Sets a password for this BGP neighbor device (or devices using this profile)</td>
<td>page 28-74</td>
</tr>
<tr>
<td>peer-group</td>
<td>Sets the peer group for this BGP neighbor device (or devices using this profile) (EXPERIMENTAL)</td>
<td>page 28-75</td>
</tr>
<tr>
<td>port</td>
<td>Configures a non-standard BGP port for this BGP neighbor (EXPERIMENTAL)</td>
<td>page 28-76</td>
</tr>
<tr>
<td>remote-as</td>
<td>Configures the ASN for this neighbor BGP device (or devices using this profile)</td>
<td>page 28-77</td>
</tr>
<tr>
<td>remove-private-as</td>
<td>Removes the private ASN from outbound updates (EXPERIMENTAL)</td>
<td>page 28-78</td>
</tr>
<tr>
<td>route-server-client</td>
<td>Enables this BGP neighbor device (or devices using this profile) to act as a route server client (EXPERIMENTAL)</td>
<td>page 28-79</td>
</tr>
<tr>
<td>send-community</td>
<td>Enables sending of the community attribute to the BGP neighbor</td>
<td>page 28-80</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down this BGP neighbor device (or devices using this profile)</td>
<td>page 28-81</td>
</tr>
<tr>
<td>soft-reconfiguration</td>
<td>Enables storing of updates for inbound soft reconfiguration</td>
<td>page 28-82</td>
</tr>
<tr>
<td>strict-capability-match</td>
<td>Enables a strict capability match before allowing a neighbor BGP peer to open a connection (EXPERIMENTAL)</td>
<td>page 28-83</td>
</tr>
<tr>
<td>timers</td>
<td>Configures this BGP neighbor’s keepalive and holdtime durations</td>
<td>page 28-84</td>
</tr>
<tr>
<td>unsuppress-map</td>
<td>Uses a route-map that selectively un suppresses routes that have been suppressed using the <code>aggregate-address</code> command</td>
<td>page 28-86</td>
</tr>
<tr>
<td>update-source</td>
<td>Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor</td>
<td>page 28-87</td>
</tr>
<tr>
<td>use</td>
<td>Configures filters for this neighbor. These filters are BGP IP ACL, IP prefix list, AS path list, and route map. Based on the filters used, updates received from this neighbor are filtered.</td>
<td>page 28-88</td>
</tr>
<tr>
<td>weight</td>
<td>Configures a weight for all routes learned from this BGP neighbor</td>
<td>page 28-89</td>
</tr>
</tbody>
</table>
28.8.1 activate

- bgp-neighbor-config commands

Enables an address family for this neighbor. This option is enabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
activate

Parameters
None

Examples
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#activate
### 28.8.2 advertisement-interval

- **bgp-neighbor-config commands**

Configures the minimum interval, in seconds, between two consecutive BGP router updates

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

advertisement-interval <0-600>

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertisement-interval &lt;0-600&gt;</td>
</tr>
</tbody>
</table>

#### Examples

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)# advertisement-interval 100

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)# show context
   bgp neighbor 192.168.13.99
   advertisement-interval 100

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

#### Related Commands

- **no**
  
  Reverts the advertisement interval to default (5 seconds)
28.8.3 allowas-in

- bgp-neighbor-config commands

Enables re-advertisement of all prefixes containing duplicate ASNs. Use this command to configure the maximum number of times an ASN is advertised. This option is disabled by default.

When enabled, Provider Edge (PE) routers can re-advertise all prefixes containing duplicate ASNs. This creates a pair of VPN Routing/Forwarding (VRF) instances on each PE router to receive and re-advertise prefixes. The PE router receives prefixes with ASNs from all PE routers and advertises to its neighbor PE routers on one VRF. The other VRF receives prefixes with ASNs from the Customer Edge (CE) routers and re-advertises them to all PE routers in the configuration.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
allowas-in <1-10>

Parameters
- allowas-in <1-10>

| allowas-in <1-10> | Enables and configures the maximum number of times an ASN is advertised.
|-------------------|--------------------------------------------------|
| <1-10>            | - Specify a value from 1 - 10.

Examples
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
allowas-in 10

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
  bgp neighbor 192.168.13.99
  advertisement-interval 100
  allowas-in 10

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

Related Commands
- no Disables re-advertisement of all prefixes containing duplicate ASNs
28.8.4 attribute-unchanged

* bgp-neighbor-config commands

Enables propagation of BGP attribute values unchanged to this neighbor BGP device. The BGP attributes are: as-path, med, and next-hop.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

attribute-unchanged { (as-path|med|next-hop) }

**Parameters**

- attribute-unchanged { (as-path|med|next-hop) }

<table>
<thead>
<tr>
<th>attribute-unchanged</th>
<th>Enables the propagation of the following BGP attribute values unchanged:</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-path - Optional.</td>
<td>Enables propagation of AS path BGP attribute unchanged to this neighbor BGP device. This option is disabled by default.</td>
</tr>
<tr>
<td>med - Optional.</td>
<td>Enables propagation of MED BGP attribute unchanged to this neighbor BGP device. This option is disabled by default</td>
</tr>
<tr>
<td>next-hop - Optional.</td>
<td>Enables propagation of the next-hop BGP attribute value unchanged to this neighbor BGP device. This option is disabled by default</td>
</tr>
</tbody>
</table>

**Examples**

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
attribute-unchanged as-path

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
   bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

**Related Commands**

no  Disables propagation of BGP attribute values unchanged to this neighbor BGP device
### 28.8.5 capability

#### bgp-neighbor-config commands

Enables the advertisement of capability (dynamic and ORF) to BGP peers.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
capability [dynamic|orf]
capability dynamic
capability orf prefix-list [both|receive|send]
```

#### Parameters

- **capability dynamic**
  - Enables the advertisement of dynamic capability
    - Enable this option to show a neighbor device's capability to advertise or withdraw and address capability to other peers in a non-disruptive manner. This option is disabled by default.

- **capability orf prefix-list [both|receive|send]**
  - Enables the advertisement of **Outbound Router Filtering** (ORF) capability. This option is disabled by default.
    - Enable this option to enable ORF, and advertise this capability to peer devices. ORFs send and receive capabilities to lessen the number of updates exchanged between BGP peers. By filtering updates, ORF minimizes update generation and exchange overhead.
    - The local BGP device advertises ORF in the `send` mode. The peer BGP device receives the ORF capability in the `receive` mode. The two devices exchange updates to maintain the ORF for each router. Only a peer group or an individual BGP router can be configured to be in `receive` or `send` mode. A peer group member cannot be configured.
      - **both** – Advertises the capability to send and receive the ORF to/from this neighbor
      - **receive** – Advertises the capability to receive the ORF from this neighbor
      - **send** – Advertises the capability to send the ORF to this neighbor

#### Examples

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)# capability orf prefix-list both

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)# show context
  bgp neighbor 192.168.13.99
  advertisement-interval 100
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
```

#### Related Commands

```
no
```
- Disables advertisement of capability (dynamic and ORF) to BGP peers
28.8.6 default-originate

▶ bgp-neighbor-config commands

Enables the sending of the default route to BGP neighbors. It also allows the configuration of the default route. When enabled and configured, local BGP routers send the default route 0.0.0.0 (or a route map specified route) to its neighbor for use as the default route.

Supported in the following platforms:

• Wireless Controllers — RFS4000, RFS6000
• Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

default-originate [route-map <BGP-ROUTE-MAP-NAME>]

Parameters

• default-originate [route-map <BGP-ROUTE-MAP-NAME>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-originate</td>
<td>Enables default originate on this BGP neighbor. This option is disabled by default.</td>
</tr>
<tr>
<td>route-map &lt;BGP-ROUTE-MAP&gt;</td>
<td>Optional. Use this keyword to specify a route map to use as the default originate route</td>
</tr>
</tbody>
</table>

Note: If no route-map is specified, the default route 0.0.0.0 is sent.

Examples

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#default-originate

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context bgp neighbor 192.168.13.99 advertisement-interval 100 allowas-in 10 attribute-unchanged as-path capability orf prefix-list both default-originate

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the sending of the default route to BGP neighbors</td>
</tr>
</tbody>
</table>
**28.8.7 description**

- **bgp-neighbor-config commands**
  Configures a description for this BGP neighbor device

  Supported in the following platforms:
  - Wireless Controllers — RFS4000, RFS6000
  - Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

  **Syntax**
  `description neighbor <LINE>`

  **Parameters**
  - `description neighbor <LINE>`

  **Examples**
  ```
  nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#description neighbor "This neighbor is an external AS neighbor"
  
  advertisement-interval 100
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
default-originate
  description neighbor "This neighbor is an external AS neighbor"
  nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
  ```

  **Related Commands**
  - `no` | Removes this BGP neighbor’s description
28.8.8 disable-connected-check

- bgp-neighbor-config commands

Enables one-hop away eBGP peer using loop back address. This option is disabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

disable-connected-check

Parameters
None

Examples

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#disable-connected-check

advertisement-interval 100
allowas-in 10
attribute-unchanged as-path
capability orf prefix-list both
default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

Related Commands

| no | Disables one-hop away eBGP peer using loop back address |
28.8.9 `dont-capability-negotiate`

- **bgp-neighbor-config commands**

   Disables capability negotiation with BGP neighbors. This is to allow compatibility with older BGP versions that have no capability parameters used in the `open` messages between peers. Capability negotiation is enabled by default.

   Supported in the following platforms:
   - Wireless Controllers — RFS4000, RFS6000
   - Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`dont-capability-negotiate`

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)##
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)##
```

**Related Commands**

- `no` Enables capability negotiation with BGP neighbors
### 28.8.10 `ebgp-multihop`

**bgp-neighbor-config commands**

Enables eBGP Multihop on this BGP neighbor. When enabled, allows neighbor connection to be established between two eBGP neighbors that are not directly connected to each other. Use this command to configure the maximum number of hops possible between two such eBGP neighbors. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
# ebgp-multihop <1-255>
```

**Parameters**

- `ebgp-multihop <1-255>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ebgp-multihop</code></td>
<td>Configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other.</td>
</tr>
<tr>
<td><code>&lt;1-255&gt;</code></td>
<td>- Specify a value from 1 - 255. The default is 255.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#ebgp-multihop 20

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
# ebgp-multihop 20
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables eBGP Multihop on this BGP neighbor</td>
</tr>
</tbody>
</table>
28.8.11 enforce-multihop

- **bgp-neighbor-config commands**
  
  Forces eBGP neighbors to perform multi-hop checks

  A *multihop* route is a route to external peers on indirectly connected networks. When enforced, eBGP neighbors perform multi-hop check. This option is disabled by default.

  Supported in the following platforms:
  - Wireless Controllers — RFS4000, RFS6000
  - Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

  **Syntax**

  `enforce-multihop`

  **Parameters**

  None

  **Examples**

  ```
  nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#enforce-multihop
  
  advertisement-interval 100
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
  enforce-multihop
  
  nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
  ```

  **Related Commands**

| **no**          | Disables enforcement of multihop route checks |
28.8.12 local-as

**bgp-neighbor-config commands**

Configures this neighbor’s local AS number

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`local-as <1-4294967295> {no-prepend}`

**Parameters**
- `local-as <1-4294967295> {no-prepend}`

<table>
<thead>
<tr>
<th>local-as &lt;1-4294967295&gt; {no-prepend}</th>
<th>Configures the local AS number</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>&lt;1-4292967295&gt;</code> – Specify a value from 1 - 4294967295.</td>
<td></td>
</tr>
<tr>
<td>• <code>no-prepend</code> – Optional. Select to enable. When enabled, the local AS number is not prepended to route updates from eBGP peers. AS numbers are prepended to route updates by default.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#local-as 20
no-prepend

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
  advertisement-interval 100
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
  dont-capability-negotiate
  ebgp-multihop 20
  enforce-multihop
  local-as 20 no-prepend
```

**Related Commands**

| `no` | Removes the local AS number. And also reverts prepending of AS numbers to default (allows prepending). |
28.8.13 maximum-prefix

* bgp-neighbor-config commands

Configures the maximum number of prefixes that can be received from a BGP neighbor. This option is disabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
maximum-prefix <1-4294967295> {(<1-100>|restart <1-65535>|warning-only)}
```

**Parameters**

- `maximum-prefix <1-4294967295>`
- `restart <1-65535>`
- `warning-only`

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#maximum-prefix 400 50 warning-only

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show con
bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
maximum-prefix 400 50 warning-only

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
```

**Related Commands**

- `no` Removes the maximum prefix settings configured for this neighbor
28.8.14 next-hop-self

Enables next-hop calculation for this neighbor. This option is disabled by default.

When enabled, this device (or devices using this profile) are configured as the next hop for the BGP speaking neighbor or peer group. This allows the BGP device to change the next hop information that is sent to iBGP peers. The next hop address is set to the IP address of the interface used to communicate with the eBGP neighbor.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`next-hop-self`

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
next-hop-self
```

```
    advertisement-interval 100
    allowas-in 10
    attribute-unchanged as-path
capability orf prefix-list both
    default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
    ebgp-multihop 20
    enforce-multihop
    local-as 20 no-prepend
    maximum-prefix 400 50 warning-only
    next-hop-self
```

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables next-hop calculation for this neighbor (this is the default)</td>
</tr>
</tbody>
</table>
28.8.15 no

*bgp-neighbor-config commands*

Removes this BGP neighbor’s settings, or reverts them back to default

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

no <PARAMETER>

**Parameters**
- no <PARAMETER>

| no <PARAMETER> | Specify the parameter details to remove or revert to default |

**Examples**

The following example shows the neighbor 192.168.13.99 settings before the ‘no’ commands are executed:

```
no 
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context bgp neighbor 192.168.13.99 advertisement-interval 100 allowas-in 10 attribute-unchanged as-path capability orf prefix-list both default-originate description neighbor "This neighbor is an external AS neighbor" disable-connected-check dont-capability-negotiate ebgp-multihop 20 enforce-multihop local-as 20 no-prepend maximum-prefix 400 50 warning-only next-hop-self
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#no advertisement-interval
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#no disable-connected-check
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#no default-originate
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#no local-as
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context bgp neighbor 192.168.13.99 allowas-in 10 attribute-unchanged as-path capability orf prefix-list both description neighbor "This neighbor is an external AS neighbor" dont-capability-negotiate ebgp-multihop 20 maximum-prefix 400 50 warning-only next-hop-self
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
```
28.8.16 **override-capability**

*bgp-neighbor-config commands*

Enables the overriding of capability negotiation results. This option is disabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

override-capability

**Parameters**

None

**Examples**

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

override-capability

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context

bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dontcapability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
override-capability

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the overriding of capability negotiation results</td>
</tr>
</tbody>
</table>
28.8.17 passive

*bgp-neighbor-config commands*

Enables this BGP neighbor device (or devices using this profile) as passive. When enabled, local devices do not attempt to open a connection to passive BGP neighbors. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
passive
```

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#passive
```

```
  advertisement-interval 100
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
  dont-capability-negotiate
  ebgp-multihop 20
  enforce-multihop
  local-as 20 no-prepend
  maximum-prefix 400 50 warning-only
  next-hop-self
  override-capability
  passive
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables this BGP neighbor device (or devices using this profile) as passive</td>
</tr>
</tbody>
</table>
28.8.18 password

Sets a password for this BGP neighbor device (or devices using this profile). When configured, this password is used for Message Digest 5 (MD5) authentication between two BGP peers connected over TCP. To enable MD5 authentication between two BGP peers, configure both with the same password.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
password neighbor <LINE>

Parameters
- password neighbor <LINE>

Examples
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#password neighbor eBGPneighbor@300

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)# show context
  bgp neighbor 192.168.13.99
  advertisement-interval 100
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
dont-capability-negotiate
ebgp-multipath 20
enforce-multipath
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the password configured for this neighbor</td>
</tr>
</tbody>
</table>
28.8.19 peer-group

Sets the peer group for this BGP neighbor device (or devices using this profile). Peer groups are a set of BGP neighbors with the same update policies. This facilitates the updates of various policies, such as, distribute lists and filter lists.

The peer group can be configured as a single entity. Any changes made to the peer group is propagated to all members.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

peer-group <PEER-GROUP-NAME>

Parameters

- peer-group <PEER-GROUP-NAME>

Examples

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#peer-group eBGPPeerGrp1

advertisement-interval 100
peer-group eBGPPeerGrp1
allowas-in 10
attribute-unchanged as-path
capability orf prefix-list both
default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive
password neighbor eBGPneighbor@300

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

Related Commands

no

Removes the peer group configuration. This neighbor peer group setting is removed.
28.8.20 port

`bgp-neighbor-config commands`

Configures a non-standard BGP port for this BGP neighbor

By default BGP uses port 179. Use this command to set a non standard port for this BGP neighbor.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
`port <0-65535>`

Parameters
- `port <0-65535>`

Examples
```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#port 21
```
```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
advertisement-interval 100
peer-group eBGPNeighbor1
   port 21
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPNeighbor@300
```

Related Commands
```
no
```
Removes the non standard port configured for this neighbor
28.8.21 remote-as

bgp-neighbor-config commands

Configures the ASN for this neighbor BGP device (or devices using this profile). ASN is a set of routers under the same administration that use Interior Gateway Protocol (IGP) and common metrics to define how to route packets within the AS.

Supported in the following platforms:
• Wireless Controllers — RFS4000, RFS6000
• Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
remote-as <1-4294967295>

Parameters
• remote-as <1-4294967295>

| remote-as <1-4294967295> | Specify the remote ASN from 1 - 4294967295. |

Examples
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#remote-as 100

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
  remote-as 100
  advertisement-interval 100
  peer-group eBGPPeerGrp1
  port 21
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
  enforce-multihop
  local-as 20 no-prepend
  maximum-prefix 400 50 warning-only
  next-hop-self
  override-capability
  passive
  password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
28.8.22 remove-private-as

- **bgp-neighbor-config commands**

Removes the private ASN from outbound updates. By default private ASNs are included in outbound updates. Private AS numbers are not advertised to the Internet. This option is used with external BGP (eBGP) peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

This option is disabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
remove-private-as
```

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
remove-private-as
```

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
remote-as 100
advertisement-interval 100
peer-group eBGPpeerGrp1
port 21
allowas-in 10
attribute-unchanged as-path
capability orf prefix-list both
default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive
password neighbor eBGPneighbor@300
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
remove-private-as
```

```
x9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Includes private ASNs in outbound updates (this is the default setting)</td>
</tr>
</tbody>
</table>
28.8.23 route-server-client

> bgp-neighbor-config commands

Enables this BGP neighbor device (or devices using this profile) to act as a route server client. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

route-server-client

Parameters

None

Examples

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
route-server-client

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
  remote-as 100
  advertisement-interval 100
  peer-group eBGGPeerGrp1
  port 21
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
  dont-capability-negotiate
  ebgp-multihop 20
  enforce-multihop
  local-as 20 no-prepend
  maximum-prefix 400 50 warning-only
  next-hop-self
  override-capability
  passive
  password neighbor eBGPneighbor@300
  remove-private-as
  route-server-client

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables this BGP neighbor device (or devices using this profile) to act as a route server client</td>
</tr>
</tbody>
</table>
28.8.24 `send-community`

`bgp-neighbor-config commands`

Enables sending of the community attribute to the BGP neighbor. The community attribute groups destinations in a certain community and applies routing decisions based on the community. On receiving community attribute, the BGP router announces it to the neighbor.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
send-community [both|extended|standard]
```

**Parameters**

- `send-community [both|extended|standard]`

| `send-community [both|extended|standard]` | Enables sending of the community attributes to the BGP neighbor |
|------------------------------------------|---------------------------------------------------------------|
|                                           | • both – Sends extended and standard community attributes     |
|                                           | • extended – Sends extended community attributes only          |
|                                           | • standard – Sends standard community attributes only          |

**Examples**

```bash
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
send-community both
```

```bash
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
  remote-as 100
  advertisement-interval 100
  peer-group eBGPPeerGrp1
  port 21
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
ebpg-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive
password neighbor eBGPneighbor@300
remove-private-as
route-server-client
  send-community both
```

**Related Commands**

<table>
<thead>
<tr>
<th><code>no</code></th>
<th>Disables sending of the community attribute to the BGP neighbor</th>
</tr>
</thead>
</table>
28.8.25 shutdown

*bgp-neighbor-config commands*

Shuts down this BGP neighbor device (or devices using this profile). When configured, this neighbor is administratively shut down. This option is disabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
shutdown
```

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#shutdown
```

```
remove-private-as
route-server-client
shutdown
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the administrative shut down of this neighbor</td>
</tr>
</tbody>
</table>
### 28.8.26 soft-reconfiguration

#### bgp-neighbor-config commands

Enables storing of updates for inbound soft reconfiguration. This option is disabled by default. Soft-reconfiguration can be used in lieu of BGP route refresh capability. Enabling this option enables local storage of all received routes and their attributes. This requires additional memory on the BGP device.

When a soft reset (inbound) is performed on the neighbor device, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
soft-reconfiguration inbound
```

#### Parameters

- `soft-reconfiguration inbound`

#### Examples

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#
soft-reconfiguration inbound
```

#### Related Commands

- `no` Disables soft reconfiguration
### 28.8.27 strict-capability-match

* bgp-neighbor-config commands

Enforces a strict capability match before allowing a TCP connection with this neighbor. In case capabilities do not match, the BGP connection is not established. This option is disabled by default.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`strict-capability-match`

**Parameters**

None

**Examples**

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#strict-capability-match

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables a strict capability match before allowing a connection with this neighbor</td>
</tr>
</tbody>
</table>
28.8.28 timers

* `bgp-neighbor-config commands`

Configures this BGP neighbor's keepalive and holdtime durations

**NOTE:** The keepalive and holdtime settings configured at the neighbor level override those configured on the BGP router.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

`timers [<0-65535> <0-65535>|connect <0-65535>]`

**Parameters**

- `timers [<0-65535> <0-65535>|connect <0-65535>]`

<table>
<thead>
<tr>
<th>timers &lt;0-65535&gt; &lt;0-65535&gt;</th>
<th>Sets the keepalive and holdtime intervals</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;0-65535&gt; – Specifies the keepalive interval from 0 - 65535 seconds. It is the interval, in seconds, between two successive keepalive packets exchanged with this neighbor to keep the TCP connection alive.</td>
<td></td>
</tr>
<tr>
<td>• &lt;0-65535&gt; – Specifies the holdtime interval from 0 - 65535. This is the time this neighbor will wait without receiving a keepalive packet from its neighbor before declaring it dead. If the time since the last keepalive packet received (from its neighbor) exceeds the value set here, the neighbor is declared dead.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>timers connect &lt;0-65535&gt;</th>
<th>Sets the BGP connect time. This is the interval, in seconds, after which BGP tries to connect to a dead peer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;0-65535&gt; – Specify a value from 1 - 65535 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#timers 20 40
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#timers connect 20
nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
  remote-as 100
  advertisement-interval 100
  peer-group eBGPPeerGrp1
  port 21
  strict-capability-match
  timers connect 20
  timers 20 40
  allowas-in 10
  attribute-unchanged as-path
  capability orf prefix-list both
  default-originate
  description neighbor "This neighbor is an external AS neighbor"
  disable-connected-check
  dont-capability-negotiate
  ebgp-multihop 20
  enforce-multihop
  local-as 20 no-prepend
  maximum-prefix 400 50 warning-only
  next-hop-self
  override-capability
  passive
```
border gateway protocol

password neighbor eBGPneighbor@300
remove-private-as
route-server-client
send-community both

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
</tr>
<tr>
<td>Removes the holdtime value set for this neighbor</td>
</tr>
</tbody>
</table>
28.8.29 unsuppress-map

- bgp-neighbor-config commands

Unsuppresses map to selectively advertise routes that have been suppressed using the aggregate-address command.

The aggregate-address command creates a route map with an IP/mask address that consolidates subnets under it. This reduces the number of route maps on the BGP device to one consolidated entry. Use unsuppress-map to selectively allow/deny a subnet or a set of subnets from this consolidated entry.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
unsuppress-map <ROUTE-MAP-NAME>

Parameters
- unsuppress-map <ROUTE-MAP-NAME>

Examples
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#
unsuppress-map test

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#show context
  bgp neighbor 192.168.13.99
  remote-as 199
  maximum-prefix 9999 80 restart 50
unsuppress-map test

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#

Related Commands
- no
  Removes the unsuppress flag applied on the specified route map
28.8.30 update-source

**bgp-neighbor-config commands**

Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

update-source <IPv4>

**Parameters**

- update-source <IPv4>

**Examples**

```
```

```
remote-as 100
advertisement-interval 100
peer-group eBGPPeerGrp1
port 21
strict-capability-match
timers connect 20
timers 20 40
allows-in 10
attribute-unchanged as-path
capability orf prefix-list both
default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive
password neighbor eBGPneighbor@300
remove-private-as
route-server-client
send-community both
update-source 192.168.13.1
```

nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#

**Related Commands**

<table>
<thead>
<tr>
<th></th>
<th>Removes the source of routing updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>
### 28.8.31 use

#### bgp-neighbor-config commands

Configures filters for this neighbor. These filters are BGP IP ACL, IP prefix list, AS path list, and route map. Based on the filters used, updates received from this neighbor are filtered.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]
```

#### Parameters

- `use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]`

#### Examples

```bash
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#
use filter-list FilterList_01 in
```

```bash
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#
use route-map testBGPRouteMap out
```

```bash
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#
show context
  bgp neighbor 192.168.13.99
  remote-as 199
  use filter-list FilterList_01 in
  maximum-prefix 9999 80 restart 50
  use route-map testBGPRouteMap out
  unsuppress-map test
```

#### Related Commands

- `no` Remoes the filters used to filter updates received from this neighbor
28.8.32 weight

bgp-neighbor-config commands

Configures a weight for all routes learned from this BGP neighbor. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The highest weight is always chosen.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
weight <0-65535>

Parameters
- weight <0-65535>

Examples
```
 nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)# weight 10
```
```
 nx9500-6C8809(config-profile testNX45XX-router-bgp-neighbor-192.168.13.99)#show context
bgp neighbor 192.168.13.99
    remote-as 100
    advertisement-interval 100
    peer-group eBGPPeerGrp1
    port 21
    strict-capability-match
    timers connect 20
    timers 20 40
    allowas-in 10
    attribute-unchanged as-path
    capability orf prefix-list both
    default-originate
    description neighbor "This neighbor is an external AS neighbor"
    disable-connected-check
    dont-capability-negotiate
    ebgp-multihop 20
    enforce-multihop
    local-as 20 no-prepend
    maximum-prefix 400 50 warning-only
    next-hop-self
    override-capability
    passive
    password neighbor eBGPneighbor@300
    remove-private-as
    route-server-client
    send-community both
    update-source 192.168.13.1
```

Related Commands
```
no
```
Reverts to default value
This chapter summarizes the crypto certificate management protocol (CMP) policy commands in the CLI command structure.

CMP is an Internet protocol designed to enable devices (access point, wireless controller, or service platform) to obtain and manage digital certificates in a Public Key Infrastructure (PKI) network. A Certificate Authority (CA) issues the certificates using the defined CMP.

WiNG CMP implementation allows you to configure a crypto CMP policy that enables auto installation and auto management of device certificates. When configured and implemented on a device, the crypto CMP policy allows the device to automatically trigger a certification request to a configured, CMP supported certificate authority (CA) server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. You can use a manually created trustpoint for one service (like HTTPS) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

Use the (config) instance to configure a crypto CMP policy. To navigate to the crypto CMP policy configuration instance, use the following commands:

```
<DEVICE>(config)#crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
ap6522-D8273A(config)#crypto-cmp-policy CMP
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#?
```

CMP Policy Mode commands:

```
csa-server         CMP CA Server configuration commands
cert-key-size      Set key size for certificate request
cert-renewal-timeout Trigger a cert renewal request on timeout
cross-cert-validate Validate cross-cert using factory-cert
no                 Negate a command or set its defaults
subjectAltName     Configure subjectAltName value
trustpoint         Trustpoint for CMP
use                Set setting to use
clrscr             Clears the display screen
commit             Commit all changes made in this session
do                 Run commands from Exec mode
end                 End current mode and change to EXEC mode
exit               End current mode and down to previous mode
help               Description of the interactive help system
revert             Revert changes
service            Service Commands
show               Show running system information
write              Write running configuration to memory or terminal
```

ap6522-D8273A(config-cmp-policy-CMP)#
This chapter is organized as follows:

- `crypto-cmp-policy-instance`
- `other-cmp-related-commands`

---

**NOTE:** The input parameter `<HOSTNAME>`, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
29.1 crypto-cmp-policy-instance

The following table summarizes crypto CMP policy configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca-server</td>
<td>Configures the CA server details</td>
<td>page 29-4</td>
</tr>
<tr>
<td>cert-key-size</td>
<td>Configures the size of the key associated with a certificate request</td>
<td>page 29-5</td>
</tr>
<tr>
<td>cert-renewal-timeout</td>
<td>Configures a certificate renewal timeout in days</td>
<td>page 29-6</td>
</tr>
<tr>
<td>cross-cert-validate</td>
<td>Enables validation of the cross certificate with the factory certificate</td>
<td>page 29-7</td>
</tr>
<tr>
<td>subjectAltName</td>
<td>Configures an alternate subject name for this CMP policy</td>
<td>page 29-8</td>
</tr>
<tr>
<td>trustpoint</td>
<td>Configures a trustpoint and its associated information, such as the subject name, the sender’s (device requesting certification) details, and the recipient’s (CA) details</td>
<td>page 29-9</td>
</tr>
<tr>
<td>use</td>
<td>Associates a device’s autogen-uniqueid with this crypto CMP policy</td>
<td>page 29-11</td>
</tr>
<tr>
<td>no</td>
<td>Removes the crypto CMP policy settings</td>
<td>page 29-12</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
29.1.1 ca-server

The CA is an external network authority (usually a trusted third-party server) that generates and issues digital certificates in response to requests received from network devices. Use this command to configure the primary and secondary CA server details, such as name of the device hosting the CA server, the port used to access the CA server, and the path where the certificate is stored. Once defined, devices using this CMP policy automatically send requests to the specified primary CA server, and retrieve the certificate from the specified location. If the primary CA server is not reachable, the requests are sent to the secondary CA server.

Supported in the following platforms:

- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
ca-server [primary|secondary] host <IP/HOSTNAME> port <PORT-NUMBER> path <PATH>
```

Parameters

- `ca-server [primary|secondary] host <IP/HOSTNAME> port <PORT-NUMBER> path <PATH>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ca-server</code></td>
<td>Configures the primary and secondary CA server details (IP address, port, and path)</td>
</tr>
<tr>
<td><code>primary</code></td>
<td>primary – Configures the primary CA server’s details</td>
</tr>
<tr>
<td><code>secondary</code></td>
<td>secondary – Configures the secondary CA server’s details</td>
</tr>
</tbody>
</table>

Note: The secondary CA is used in case the primary CA server is not reachable. CA server settings are required to complete CMP requests.

`host <IP/HOSTNAME>`

- Configures IP address or hostname of the device hosting the primary/secondary CA server
- `<IP/HOSTNAME>` – Specify the IP address or hostname.

`port <PORT-NUMBER>`

- Configures the port on which the primary/secondary CA server can be reached
- `<PORT-NUMBER>` – Specify the port number.

`path <PATH>`

- Configures the path or filename of the primary/secondary CA certificate. Enter the complete relative path to the file on the server.
- `<PATH>` – Specify the path. Once specified, the certificate is downloaded from this location and installed on the device.

Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#ca-server primary host 192.168.8.74 port 8 path cmp
```

```
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
crypto-cmp-policy
```

```
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

- `no`

  Removes the configured primary/secondary CA server details
29.1.2 **cert-key-size**

- **crypto-cmp-policy-instance**

Configures the size of the key associated with a certificate request.

Supported in the following platforms:

- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

cert-key-size [2048|3072|4096]

**Parameters**

- cert-key-size [2048|3072|4096]

| cert-key-size [2048|3072|4096] | Configures the certificate request key size. The options are: |
|----------------------------------|------------------------------------------------------------|
| 2048                            | • 2048 – Sets the key size to 2048 bits. This is the default setting. |
| 3072                            | • 3072 – Sets the key size to 3072 bits |
| 4096                            | • 4096 – Sets the key size to 4096 bits |

**Examples**

nx9500-6C8809(config-cmp-policy-test)#cert-key-size 3072

nx9500-6C8809(config-cmp-policy-test)#show context
crypto-cmp-policy test
  cert-key-size 3072
trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 2
osr2bwjR+0L+G64ny3wfuAAAAAtTFjeFvOixTHLDfgt7Bu reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
nx9500-6C8809(config-cmp-policy-test)#

**Related Commands**

- **no** Reverts the certificate request key size to default (2048 bits)
29.1.3 cert-renewal-timeout

`crypto-cmp-policy-instance`

Configures a certificate renewal timeout in days. This is the number of days, before the expiration of the device’s certificate, that a certificate renewal is triggered.

The expiration of device’s certificate is checked once a day. When a certificate is about to expire a certificate renewal is initiated with the dedicated CMP CA server resource through an existing IPSec tunnel. If the tunnel is not established, the CMP renewal request is not sent. If a renewal succeeds the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

Supported in the following platforms:
- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
cert-renewal-timeout <1-60>
```

**Parameters**
- `cert-renewal-timeout <1-60>`

<table>
<thead>
<tr>
<th>cert-renewal-timeout</th>
<th>Configures the certificate renewal timeout in days. This is the number of days, before the expiration of the device’s certificate, that a certificate renewal is triggered. Once the configured time is completed, the device triggers a certificate renewal request.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-60&gt;</td>
<td>• &lt;1-60&gt; — Specify a value from 1 - 60 days. The default is fourteen (14) days. Therefore, by default a device triggers certificate renewal request 14 days before its certificate expires.</td>
</tr>
</tbody>
</table>

**Examples**
```
ap6522-D8273A(config-cmp-policy-CMP)#cert-renewal-timeout 60

ap6522-D8273A(config-cmp-policy-CMP)#show context crypto-cmp-policy CMP
cert-renewal-timeout 60
ca-server primary host 192.168.8.74 port 8 path cmp
ap6522-D8273A(config-cmp-policy-CMP)#
```

**Related Commands**
```
no                   Reverts the certificate renewal timeout to default (14 days)
```
29.1.4 cross-cert-validate

* crypto-cmp-policy-instance

Enables validation of the cross certificate using the factory certificate. When enabled, the obtained cross-certificate is validated against the operator’s certificate configured using the `trustpoint > cmp-auth-operator` command. An error message is displayed in case the cross-certificate is not obtained or if the cross-certificate is found to be invalid. This option is disabled by default.

**NOTE:** To the operator certificate, in the device configuration mode execute the `trustpoint > cmp-auth-operator` command. For more information, see `trustpoint (device-config-mode)`.

Supported in the following platforms:
- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
cross-cert-validate

**Parameters**
None

**Examples**
nx9500-6C8809(config-cmp-policy-test)#cross-cert-validate

nx9500-6C8809(config-cmp-policy-test)#show context crypto-cmp-policy test
    cert-key-size 3072
cross-cert-validate
    trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 2 9piuK/GqvD+G64ny3wfA AAAAvqCi8WjkNjpryMD9IAPk4T reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company, CN=ExampleCompany.com" recipient-name "O=Example Company, CN=ExampleCompany.com"
nx9500-6C8809(config-cmp-policy-test)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables validation of the cross certificate with the factory certificate</td>
</tr>
</tbody>
</table>
29.1.5 subjectAltName

*crypto-cmp-policy-instance*

Configures the subjectAltName identity for this CMP policy

Supported in the following platforms:
- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn <FQDN>|string <USER-DEFINED-STRING>]
```

**Parameters**

- `subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn <FQDN>|string <USER-DEFINED-STRING>]`

<table>
<thead>
<tr>
<th>subjectAltName [address &lt;IP&gt;]</th>
<th>dn &lt;DISTINGUISHED-NAME&gt;</th>
<th>email &lt;EMAIL-ID&gt;</th>
<th>fqdn &lt;FQDN&gt;</th>
<th>string &lt;USER-DEFINED-STRING&gt;</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the subjectAltName identity using one of the following options:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• address &lt;IP&gt; – Uses IP address as identity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• &lt;IP&gt; – Specify the IP address.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• dn &lt;DISTINGUISHED-NAME&gt; – Uses distinguished name as identity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• &lt;DISTINGUISHED-NAME&gt; – Specify the DISTINGUISHED-NAME.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• email &lt;EMAIL-ID&gt; – Uses e-mail address as identity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• &lt;EMAIL-ID&gt; – Specify the e-mail address.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• fqdn &lt;FQDN&gt; – Uses FQDN as identity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• &lt;FQDN&gt; – Specify the FQDN.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• string &lt;USER-DEFINED-STRING&gt; – Uses a user specified name as identity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• &lt;USER-DEFINED-STRING&gt; – Specify the string to use as identity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
ap6522-D8273A(config-cmp-policy-CMP)#subjectAltName dn TechPubsCA
```  
```
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
  cert-update
cert-renewal-timeout 60
csa-server primary host 192.168.8.74 port 8 path cmp
subjectAltName dn TechPubsCA
```  
```
ap6522-D8273A(config-cmp-policy-CMP)#
```

**Related Commands**

- `no` Removes the subjectAltName identity configured with this CMP policy
### 29.1.6 trustpoint

**crypto-cmp-policy-instance**

Configures a trustpoint and its associated information, such as the subject name, the sender's (device requesting certification) details, and the recipient's (CA) details. This information is needed to obtain the certificate from the CA server using CMP.

Each certificate is digitally signed by a *trustpoint* and contains device-specific information, such as device name, IP address, serial number. It helps to uniquely identify a device.

Supported in the following platforms:
- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
trustpoint <TRUSTPOINT-NAME> subject-name <WORD> secret [0 <WORD>|2 <WORD>] reference-id <WORD> sender-name <WORD> [recipient-name <WORD>|ca-psk <CERT-PATH>]
```

#### Parameters

- **trustpoint <TRUSTPOINT-NAME> subject-name <WORD> secret [0 <WORD>|2 <WORD>] reference-id <WORD> sender-name <WORD> [recipient-name <WORD>|ca-psk <CERT-PATH>]**

<table>
<thead>
<tr>
<th>trustpoint &lt;TRUSTPOINT-NAME&gt;</th>
<th>Configures a trustpoint name (should not exceed 32 characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>subject-name &lt;WORD&gt;</td>
<td>Configures a subject name for this trustpoint. The subject name should uniquely identify the certificate and should not exceed 512 characters in length.</td>
</tr>
<tr>
<td>secret [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]</td>
</tr>
<tr>
<td>reference-id &lt;WORD&gt;</td>
<td>Configures the reference ID. The CA server uses this information to identify the shared secret key used.</td>
</tr>
<tr>
<td>sender-name &lt;WORD&gt;</td>
<td>Configures the sender's name. The CA server uses this information to identify the shared secret key used. The sender’s name should not exceed 512 characters in length.</td>
</tr>
<tr>
<td>recipient-name</td>
<td>Configures the recipient's name. The CA server uses this information to validate the request. The recipient's name should not exceed 256 characters in length.</td>
</tr>
<tr>
<td>ca-psk &lt;CERT-PATH&gt;</td>
<td>Configures the certificate path for the server certificate</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configures a clear text password</td>
</tr>
<tr>
<td></td>
<td>Configures an encrypted password</td>
</tr>
<tr>
<td></td>
<td>Specify the reference ID.</td>
</tr>
<tr>
<td></td>
<td>Specify the sender name.</td>
</tr>
<tr>
<td></td>
<td>Specify the certificate path.</td>
</tr>
</tbody>
</table>
Examples

ap6522-D8273A(config-cmp-policy-CMP)#trustpoint cmp-test subject-name "CN=Example Company, O=Example Company" secret 0 test-secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#show context crypto-cmp-policy CMP
cert-update
cert-renewal-timeout 60
ca-server primary host 192.168.8.74 port 8 path cmp trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the trustpoint associated with this crypto CMP policy</td>
</tr>
</tbody>
</table>
29.1.7 use

* crypto-cmp-policy-instance

Associates a device’s autogen-uniqueid with this crypto CMP policy

A device’s autogen-uniqueid is a combination of a user-defined string (prefix or suffix) and a substitution token. The WiNG software implementation provides two built-in substitution tokens: $SN and $MiNT-ID that represent the device’s serial number and MiNT ID respectively. These substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for a device.

To auto generate the device’s unique ID, in the device configuration mode execute the following command:

```
autogen-uniqueid <WORD>
```

For more information on the autogen-uniqueid command, see `autogen-uniqueid`.

Supported in the following platforms:

- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```text
use autogen-uniqueid
```

Parameters

- **use autogen-uniqueid**

<table>
<thead>
<tr>
<th>command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use autogen-uniqueid</td>
<td>Associates a device’s autogen-uniqueid with this crypto CMP policy. The device’s autogen-uniqueid should be existing and configured.</td>
</tr>
</tbody>
</table>

Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#use autogen-uniqueid

ap6522-D8273A(config-cmp-policy-CMP)#show context crypto-cmp-policy
  cert-update
  cert-renewal-timeout 60
  use autogen-uniqueid
  ca-server primary host 192.168.8.74 port 8 path cmp
  trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-secret
  reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company"
  recipient-name "O=Example Company, CN=ExampleCompany.com"
  subjectAltName dn TechPubsCA

ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

```
no
```

Removes the device’s autogen-uniqueid associated with this crypto CMP policy
29.1.8 no

- crypto-cmp-policy-instance

Removes or reverts this crypto CMP policy settings

Supported in the following platforms:

- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [ca-server <SERVER-NAME>|cert-key-size|cert-renewal-timeout|cross-cert-validate|subjectAltName|trustpoint <TRUSTPOINT-NAME>|use autogen-uniqueid]

Parameters

- no <PARAMETERS>

Examples

ap6522-D8273A(config-cmp-policy-CMP)#show context
cert-update
cert-renewal-timeout 60
use autogen-uniqueid
ca-server primary host 192.168.8.74 port 8 path cmp
cert-update
trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-secret reference-id cmp-test subject-name "CN=ExampleCompany.com, O=Example Company"
recipient-name "O=Example Company, CN=ExampleCompany.com"
sender-name "CN=ExampleCompany.com, O=Example Company"
sender-name "CN=ExampleCompany.com, O=Example Company"
subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#

ap6522-D8273A(config-cmp-policy-CMP)#no cert-renewal-timeout
ap6522-D8273A(config-cmp-policy-CMP)#no subjectAltName

ap6522-D8273A(config-cmp-policy-CMP)#show context
cert-update
use autogen-uniqueid
ca-server primary host 192.168.8.74 port 8 path cmp
trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-secret reference-id cmp-test subject-name "CN=ExampleCompany.com, O=Example Company"
recipient-name "O=Example Company, CN=ExampleCompany.com"
recipient-name "O=Example Company, CN=ExampleCompany.com"
sender-name "CN=ExampleCompany.com, O=Example Company"
sender-name "CN=ExampleCompany.com, O=Example Company"
subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
29.2 other-cmp-related-commands

The following table summarizes other commands associated with the implementation of the crypto CMP policy:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>Associates a crypto CMP policy with a device</td>
<td>page 29-14</td>
</tr>
<tr>
<td>show</td>
<td>Displays current status of CMP requests in progress. This command also displays trustpoint details (CMP and non-CMP trustpoints).</td>
<td>page 29-15</td>
</tr>
</tbody>
</table>
29.2.1 use

Applies a crypto CMP policy to a device. Once CMP enabled, the device automatically requests for a certificate from the CA server and installs it. After applying the CMP policy, commit and write the change to memory. This is needed to apply this configuration across reboots.

To apply a CMP policy on a device, navigate to the device’s config-device mode and execute the `use > crypto-cmp-policy > <CRYPTO-CMP-POLICY-NAME>` command.

Supported in the following platforms:

- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

**Parameters**

- `use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>`

---

<table>
<thead>
<tr>
<th>cmp-policy &lt;CRYPTO-CMP-POLICY-NAME&gt;</th>
<th>Applies an existing crypto CMP policy on this device. When associated with a profile, the crypto CMP policy is applied to all devices using the profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;CRYPTO-CMP-POLICY-NAME&gt; – Specify the crypto CMP policy name. Should be existing and configured.</td>
</tr>
</tbody>
</table>

**Examples**

```
ap6522-D8273A(config-device-00-11-3F-D8-27-3A)#use crypto-cmp-policy CMP
ap6522-D8273A(config-device-00-11-3F-D8-27-3A)#commit
```
29.2.2 show

other-cmp-related-commands
Displays current status of CMP requests in progress. This command also displays trustpoint details (CMP and non-CMP trustpoints).

Supported in the following platforms:
- Access Points — AP622, AP650, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, WiMod
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax
show crypto [cmp|pki]
show crypto cmp request status
display crypto pki trustpoints

Parameters
- show crypto cmp request status
- show crypto pki trustpoints

Examples
ap6522-D8273A#show crypto pki trustpoints
---------------------------------------------------------------------------------------
TRUSTPOINT            KEY NAME                  VALID UNTIL
---------------------------------------------------------------------------------------
cmp-test              cmp-test-key               Fri May 9 09:44:22 2014 GMT
default-trustpoint    default_rsa_key          Fri Dec 30 00:00:40 2022 GMT
---------------------------------------------------------------------------------------
ap6522-D8273A#
ap6522-D8273A(config)#show crypto cmp request status
CMP Request Status:   cmp-complete

ap6522-D8273A#
This chapter summarizes the Roaming Assist policy commands in the CLI command structure.

By constantly monitoring a client's packets and the *received signal strength indicator* (RSSI) of a given client by a group of access points, decision can be made on the optimal access point to which the client needs to roam. Then forcefully direct the client to the optimal access point.

The threshold intervals are configurable and can be adjusted based on the client load.

Use the (config) instance to configure a Roaming Assist policy. To navigate to the Roaming Assist policy configuration instance, use the following commands:

```plaintext
<DEVICE> (config) roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>
```

```plaintext
nx9500-6C8809(config)roaming-assist-policy test
```

```plaintext
nx9500-6C8809(config-roaming-assist-policy-test)#?
```

Roaming Assist Mode commands:

- **action** Configure action - action is deauth / log / assisted-roam
- **aggressiveness** Configure the roaming aggressiveness for a wireless client
- **detection-threshold** Configure the detection threshold - when exceeded, client monitoring starts
- **disassoc-time** Configure the disassociation time - time after which a disassociation is sent
- **handoff-count** Configure the handoff count - number of times client can exceed handoff threshold
- **handoff-threshold** Configure the handoff threshold - when exceeds an action is taken.
- **monitoring-interval** Configure the monitoring interval - interval at which client monitoring occurs
- **no** Negate a command or set its defaults
- **sampling-interval** Configure the sampling interval - interval at which client rssi values are checked
- **clrscr** Clears the display screen
- **commit** Commit all changes made in this session
- **end** End current mode and change to EXEC mode
- **exit** End current mode and down to previous mode
- **help** Description of the interactive help system
- **revert** Revert changes
- **service** Service Commands
- **show** Show running system information
- **write** Write running configuration to memory or terminal

```plaintext
nx9500-6C8809(config-roaming-assist-policy-test)#
```
NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.
30.1 roaming-assist-policy-instance

The following table summarizes roaming assist policy configuration mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Specifies the action to be invoked on the client</td>
<td>page 30-4</td>
</tr>
<tr>
<td>aggressiveness</td>
<td>Configures a roaming aggressiveness value for wireless clients</td>
<td>page 30-5</td>
</tr>
<tr>
<td>detection-</td>
<td>Configures the detection-threshold value</td>
<td>page 30-6</td>
</tr>
<tr>
<td>threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>disassoc-time</td>
<td>Configures the disassociation interval</td>
<td>page 30-7</td>
</tr>
<tr>
<td>handoff-count</td>
<td>Configures the handoff-count value</td>
<td>page 30-8</td>
</tr>
<tr>
<td>handoff-</td>
<td>Configures the handoff-threshold value</td>
<td>page 30-9</td>
</tr>
<tr>
<td>threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>monitoring-</td>
<td>Configures the client monitoring interval</td>
<td>page 30-10</td>
</tr>
<tr>
<td>interval</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sampling-interval</td>
<td>Configures the interval at which clients are sampled to determine their RSSI value</td>
<td>page 30-11</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts this roaming assist policy settings based on the parameters passed</td>
<td>page 30-12</td>
</tr>
</tbody>
</table>

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Chapter 5, COMMON COMMANDS.
30.1.1 action

roaming-assist-policy-instance

Specifies the action invoked on the client once it reaches a specified threshold value. The threshold values are configured based on the client load.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

action [assisted-roam|deauth|log]

Parameters

- action [assisted-roam|deauth|log]

| action [assisted-roam|deauth|log] | Configures the action invoked on the client once it reaches the specified threshold value. The options are:
|--------------------------------------|--------------------------------------------------|
| • assisted-roam – Provides 802.11v assisted roaming facility to the client
| • deauth – De-authenticates the client. This is the default setting.
| • log – Generates a log
| In all three cases an event is generated. However, the message generated differs and is based on the action specified.

Examples

rfs6000-81742D(config-roaming-assist-policy-test)#action log
rfs6000-81742D(config-roaming-assist-policy-test)#

Related Commands

- no | Removes the configured action details
### 30.1.2 aggressiveness

Configures a roaming aggressiveness value for wireless clients. Configuring this value increases the client's roaming capabilities in scenarios where the client's location is likely to change drastically and suddenly. For example, when a client hops on to a train that speeds up quickly. In such a scenario, the access point receives a maximum of 2 (two) messages, from the client, having relatively low RSSI value. This results in a decaying-average, which is above the specified handover-threshold value. Consequently, the client is unable to roam.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
aggressiveness [highest|lowest|medium|medium-high|medium-low]
```

**Parameters**
- `aggressiveness [highest|lowest|medium|medium-high|medium-low]`

| aggressiveness [highest|lowest|medium|medium-high|medium-low] | Configures a roaming aggressiveness value for wireless clients. The options are:
| | • highest – De-authenticates client in case of any degradation in the client's link quality. When selected, the access point considers only the RSSI value of the last message received from the client.
| | • lowest – De-authenticates client only in case of significant degradation in the client's link quality. When selected, the access point uses a weighted average [80% of decaying average + 20% of last seen RSSI] as the final reported RSSI value. This is the default setting.
| | • medium – This is an intermediate setting between not roaming and performance
| | • medium-high – Allows roaming even if performance goes down. When selected, the access point calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the last received value.
| | • medium-low – Allows roaming even if performance goes average. When selected, the access point calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the average value.

**Examples**

```
nx9500-6C8809(config-roaming-assist-policy-test)#aggressiveness medium
```

```
nx9500-6C8809(config-roaming-assist-policy-test)#show context roaming-assist-policy-test aggressiveness medium
```

```
nx9500-6C8809(config-roaming-assist-policy-test)#
```

**Related Commands**

- `no` Reverts the aggressiveness value to default (lowest)
30.1.3 **detection-threshold**

Specifies the detection-threshold determining when a client is monitored

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**
detection-threshold <-100--40>

**Parameters**

- detection-threshold <-100--40>

<table>
<thead>
<tr>
<th>detection-threshold</th>
<th>Configures the detection threshold value determining when a client is monitored. The clients with bad RSSI values are monitored more frequently.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;-100--40&gt;</td>
<td>- Specify the RSSI value from -100 dBm - -40 dBm. The default is -75 dBm.</td>
</tr>
</tbody>
</table>

**Examples**

rfs6000-81742D(config-roaming-assist-policy-test)#detection-threshold -90
rfs6000-81742D(config-roaming-assist-policy-test)#

**Related Commands**

- **no** Removes the configured detection threshold details
30.1.4 disassoc-time

roaming-assist-policy-instance

Configures the disassociation time. This is the time period after which a disassociation message is sent.

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

```
disassoc-time <1-10>
```

Parameters

- disassoc-time <1-10>

<table>
<thead>
<tr>
<th>disassoc-time &lt;1-10&gt;</th>
<th>Configures the disassociation time in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-10&gt;</td>
<td>• &lt;1-10&gt; – Specify a value from 1 - 10 seconds. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#disassoc-time 7
```

```
nx9500-6C8809(config-roaming-assist-policy-test)#show context roaming-assist-policy test
disassoc-time 7
```

```
nx9500-6C8809(config-roaming-assist-policy-test)#
```

Related Commands

- no

Removes the configured disassociation time
### 30.1.5 handoff-count

**roaming-assist-policy-instance**

Specifies the number of times a client can exceed the specified handoff-threshold value before an action is invoked.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
handoff-count <1-10>
```

**Parameters**

- `handoff-count <1-10>`

**Examples**

```plaintext
rfs6000-81742D(config-roaming-assist-policy-test)#handoff-count 1
rfs6000-81742D(config-roaming-assist-policy-test)#
```

**Related Commands**

- `no` Removes the configured handoff-count details
### 30.1.6 **handoff-threshold**

> **roaming-assist-policy-instance**

Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
handoff-threshold <-100--40>
```

**Parameters**

- `handoff-threshold <-100--40>`

<table>
<thead>
<tr>
<th>handoff-threshold &lt;-100--40&gt;</th>
<th>Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;-100--40&gt;</code> – Specify the RSSI value from -100 dBm - -40 dBm. The default is -80 dBm. If the client's RSSI increases beyond the set handoff-threshold, it is removed from the queue for monitoring and action invocation.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs6000-81742D(config-roaming-assist-policy-test)#handoff-threshold -78
rfs6000-81742D(config-roaming-assist-policy-test)#
```

**Related Commands**

```
no
```

Removes the configured handoff-threshold details
30.1.7 monitoring-interval

roaming-assist-policy-instance

Configures the interval, in seconds, at which clients are monitored to determine if their RSSI value is below the specified handoff-threshold value

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

monitoring-interval <1-60>

Parameters

- monitoring-interval <1-60>

<table>
<thead>
<tr>
<th>monitoring interval &lt;1-60&gt;</th>
<th>Specifies the interval, in seconds, at which clients are monitored to determine if their RSSI is below the specified handoff-threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-60&gt; – Specify the duration from 1 - 60 seconds. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

Examples

rfs6000-81742D(config-roaming-assist-policy-test)#monitoring-interval 10
rfs6000-81742D(config-roaming-assist-policy-test)#

Related Commands

- no Removes the configured monitoring interval details
30.1.8 sampling-interval

roaming-assist-policy-instance

Configures the interval, in seconds, at which clients are sampled to determine their RSSI value.

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

sampling-interval <5-60>

Parameters

- sampling-interval <5-60>

<table>
<thead>
<tr>
<th>sampling-interval &lt;5-60&gt;</th>
<th>Configures the interval, in seconds, between two successive client samplings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;5-60&gt;</td>
<td>&lt;5-60&gt; – Specify a value from 5 - 60 seconds. The default value is 15 seconds.</td>
</tr>
</tbody>
</table>

**Note:** Higher the RSSI value, stronger is the signal.

Examples

rfs6000-81742D(config-roaming-assist-policy-test)#sampling-interval 20
rfs6000-81742D(config-roaming-assist-policy-test)#

Related Commands

- no

Removes the configured sampling interval details.
30.1.9 no

roaming-assist-policy-instance

Removes or reverts this roaming assist policy settings based on the parameters passed

Supported in the following platforms:

- Access Points — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, NX7510, NX7520, NX7530, NX9000, NX9500, NX9510, NX9600

Syntax

no [action|aggressiveness|detection-threshold|disassoc-time|handoff-count|handoff-threshold|monitoring-interval|sampling-interval]

Parameters

- no <PARAMETERS>

no <PARAMETERS> Removes or reverts this roaming assist policy settings to default based on the parameters passed

Examples

rfs6000-81742D(config-roaming-assist-policy-test)#no action
rfs6000-81742D(config-roaming-assist-policy-test)#no detection-threshold
rfs6000-81742D(config-roaming-assist-policy-test)#no handoff-threshold
rfs6000-81742D(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
  sampling-interval 20
  monitoring-interval 10
rfs6000-81742D(config-roaming-assist-policy-test)#
APPENDIX A
CONTROLLER MANAGED WLAN USE CASE

This section describes the activities required to configure a WLAN. Instructions are provided using the wireless controller CLI.

• Creating a First Controller Managed WLAN
  • Assumptions
  • Design
  • Using the Command Line Interface to Configure the WLAN
A.1 Creating a First Controller Managed WLAN

**CONTROLLER MANAGED WLAN USE CASE**
This section describes the process of creating managed WLAN on an RFS4000 wireless controller.
Upon completion, you will have created a WLAN on a RFS4000 model wireless controller using a DHCP server to allocate IP addresses to associated wireless clients.

### A.1.1 Assumptions
Verify the following conditions have been satisfied before attempting the WLAN configuration activities described in this section:

- It is assumed the RFS4000 wireless controller has the latest firmware version available.
- It is assumed the AP650 and AP71XX access points also have the latest firmware version available.
- It is assumed there are no previous configurations on the wireless controller or access point and default factory configurations are running on the devices.
- It is assumed you have administrative access to the wireless controller and access point CLI.
- It is assumed the individual administrating the network is a professional network installer.

### A.1.2 Design
This section defines the network design being implemented.

![Figure A-1 Network Design](image)

This is a simple deployment scenario, with the access points connected directly to the wireless controller. One wireless controller port is connected to an external network.

On the RFS4000 wireless controller, the GE1 interface is connected to an external network. Interfaces GE3 and GE4 are used by the access points.

On the external network, the wireless controller is assigned an IP address of 192.168.10.188. The wireless controller acts as a DHCP server for the wireless clients connecting to it, and assigns IP addresses in the range of 172.16.11.11 to 172.16.11.200. The rest of IPs in the range are reserved for devices requiring static IP addresses.
A.1.3 Using the Command Line Interface to Configure the WLAN

Creating a First Controller Managed WLAN

These instructions are for configuring your first WLAN using the wireless controller CLI.

Use a serial console cable when connecting to the wireless controller for the first time. Set the following configuration when using the serial connection:

- Bits per second: 19200
- Data Bit: 8
- Parity: None
- Stop Bit: 1
- Flow Control: None

The steps involved in creating a WLAN on a wireless controller are:

1. **Logging Into the Controller for the First Time**
2. **Creating a RF Domain**
3. **Creating a Wireless Controller Profile**
4. **Creating an AP Profile**
5. **Creating a DHCP Server Policy**
6. **Completing and Testing the Configuration**

A.1.3.1 Logging Into the Controller for the First Time

Using the Command Line Interface to Configure the WLAN

When powering on the wireless controller for the first time, you are prompted to replace the existing administrative password. The credentials for logging into the wireless controller for the first time are:

- User Name: admin
- Password: admin123

Ensure the new password created is strong enough to provide adequate security for the wireless controller managed network.

A.1.3.2 Creating a RF Domain

Using the Command Line Interface to Configure the WLAN

A RF Domain is a collection of configuration settings specific to devices located at the same physical deployment, such as a building or a floor. Create a RF Domain and assign the country code where the devices are deployed. This is a mandatory step, and the devices will not function as intended if this step is omitted.

The instructions in this section must be performed from the Global Configuration mode of the wireless controller. To navigate to this mode:

```
rfs4000>enable
rfs4000#
rfs4000#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
rfs4000(config)#
```
Create the RF Domain using the following commands:

```plaintext
rfs4000(config)#rf-domain RFDOMAIN_UseCase1
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#
```

This command creates a profile with the name `RFDOMAIN_UseCase1`.

Set the country code for the RF Domain.

```plaintext
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#country-code us
```

This sets the country code for this RF Domain. Save this change and exit the RF Domain profile context.

```plaintext
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#commit write
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#exit
rfs4000(config)#
```

To define the wireless controller’s physical location, use the same RF Domain configuration.

```plaintext
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use rf-domain RFDOMAIN_UseCase1
```

Commit the changes and write to the running configuration. Exit this context.

```plaintext
rfs4000(config-device-03-14-28-57-14-28)#commit write
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#
```

### A.1.3.3 Creating a Wireless Controller Profile

#### Using the Command Line Interface to Configure the WLAN

The first step in creating a WLAN is to configure a profile defining the parameters applied to a wireless controller.

To create a profile:

```plaintext
rfs4000(config)#profile rfs4000 RFS4000_UseCase1
rfs4000(config-profile-RFS4000_UseCase1)#
```

This creates a profile with the name `RFS4000_UseCase1` and moves the cursor into its context. Any configuration made under this profile is available when it is applied to a device.

**Configure a VLAN**

Create the VLAN to use with the WLAN configuration. This can be done using the following commands:

```plaintext
rfs4000(config-profile-RFS4000_UseCase1)#interface vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#ip address 172.16.11.1/24
```

The above command assigns the IP address 172.16.11.1 with the mask of 255.255.255.0 to VLAN 2. Exit the VLAN 2 context.

```plaintext
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

The next step is to assign this newly created VLAN to a physical interface. In this case, VLAN 2 is mapped to GE3 and GE4 to support two access points, an AP650 and an AP71XX. The AP650 is connected to the gigabit interface GE3 and the AP71XX to the GE4 interface.

```plaintext
rfs4000(config-profile-RFS4000_UseCase1)#interface ge 3
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#
```

**Map VLAN 2 to this interface. This assigns the IP address to the selected physical interface.**

```plaintext
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

Similarly, map the defined VLAN 2 to the GE4 interface.

```plaintext
rfs4000(config-profile-RFS4000_UseCase1)#interface ge 4
rfs4000(config-profile-RFS4000_UseCase1-if-ge4)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge4)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

Exit the profile and save it.

```plaintext
rfs4000(config-profile-RFS4000_UseCase1)#exit
rfs4000(config)#commit write
```
Configure the Wireless Controller to use the Profile

Before the wireless controller can be further configured, the profile must be applied to the wireless controller.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use profile RFS4000_UseCase1
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#commit write
```

Create a WLAN

Use the following commands to create a WLAN:

```
rfs4000(config)#wlan 1
rfs4000(config-wlan-1)#
```

Configure the SSID for the WLAN. This is the value that identifies and helps differentiate this WLAN.

```
rfs4000(config-wlan-1)#ssid WLAN_USECASE_01
```

Enable the SSID to be broadcast so wireless clients can find it and associate.

```
rfs4000(config-wlan-1)#broadcast-ssid
```

Associate VLAN 2 to the WLAN and exit.

```
rfs4000(config-wlan-1)#vlan 2
rfs4000(config-wlan-1)#exit
```

Commit the Changes

Once these changes have been made, they have to be committed before proceeding.

```
rfs4000(config)#commit write
```

A.1.3.4 Creating an AP Profile

Using the Command Line Interface to Configure the WLAN

An AP profile provides a method of applying common settings to access points of the same model. The profile significantly reduces the time required to configure access points within a large deployment. For more information, see:

- Creating an AP650 Profile
- Creating an AP71XX Profile

A.1.3.4.1 Creating an AP650 Profile

Creating an AP Profile

An AP650’s firmware is updated directly by its associated wireless controller. The process is automatic, and no intervention is required. To create a profile for use with an AP650:

```
rfs4000(config)#profile ap650 AP650_UseCase1
rfs4000(config-profile-AP650_UseCase1)#
```

Assign the access point to be a member of the same VLAN defined in Creating an AP Profile on page A-5. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of VLAN 2.

```
rfs4000(config-profile-AP650_UseCase1)#interface vlan 2
rfs4000(config-profile-AP650_UseCase1-if-vlan2)#
```

Configure this VLAN to use DHCP, so any device that is associated using this access point is automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-AP650_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-AP650_UseCase1-if-vlan2)#exit
```

The VLAN has to be mapped to a physical interface on the access point. Since the only available physical interface on the AP650 is GE1, this VLAN is mapped to it.

```
rfs4000(config-profile-AP650_UseCase1)#interface ge 1
rfs4000(config-profile-AP650_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-AP650_UseCase1-if-ge1)#exit
```

Before a WLAN can be implemented, it has to be mapped to a radio on the access point. An AP650 has 2 radios, in this scenario, both radios are utilized.
A.1.3.4.2 Creating an AP71XX Profile

Creating an AP Profile

To create a profile for use with an AP71XX:

```
rfs4000(config)#profile ap7131 AP7131_UseCase1
rfs4000(config-profile-AP7131_UseCase1)#
```

Set the access point to be a member of the same VLAN defined in Creating an AP Profile on page A-5. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of the VLAN 2.

```
rfs4000(config-profile-AP7131_UseCase1)#interface vlan 2
rfs4000(config-profile-AP7131_UseCase1-if-vlan2)#
```

Configure this VLAN to use DHCP, so any device associated using this access point is automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-AP7131_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-AP7131_UseCase1-if-vlan2)#exit
```

The configured VLAN has to be mapped to a physical interface on the access point. Map VLAN 2 to the GE1 and GE2 interfaces on the AP71XX. To configure the GE1 interface:

```
rfs4000(config-profile-AP7131_UseCase1)#interface ge 1
rfs4000(config-profile-AP7131_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-AP7131_UseCase1-if-ge1)#exit
```

Similarly configure the GE2 interface.

```
rfs4000(config-profile-AP7131_UseCase1)#interface ge 2
rfs4000(config-profile-AP7131_UseCase1-if-ge2)#switchport access vlan 2
rfs4000(config-profile-AP7131_UseCase1-if-ge2)#exit
```

Before the WLAN can be implemented, it has to be mapped to the physical radio on the access point. An AP71XX has 3 radios (on certain models), two of which can be configured for WLAN support. In this scenario, two radios are used.

```
rfs4000(config-profile-AP7131_UseCase1)#interface radio 1
rfs4000(config-profile-AP7131_UseCase1-if-radio1)#wlan 1
```
CONTROLLER MANAGED WLAN USE CASE A-7

rfs4000(config-profile-AP7131_UseCase1-if-radio1)#exit
rfs4000(config-profile-AP7131_UseCase1)#interface radio 2
rfs4000(config-profile-AP7131_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-AP7131_UseCase1-if-radio2)#exit
rfs4000(config-profile-AP7131_UseCase1)#

Commit the changes made to the profile and exit this context.

rfs4000(config-profile-AP7131_UseCase1)#commit write
rfs4000(config-profile-AP7131_UseCase1)#exit
rfs4000(config)#

Apply this Profile to the Discovered AP71XX

Access the discovered access point using the following command. The discovered device’s MAC address is used to access its context.

rfs4000(config)#ap7131 00-23-68-16-C6-C4
rfs4000(config-device-00-23-68-16-C6-C4)#

Assign the AP profile to this access point.

rfs4000(config-device-00-23-68-16-C6-C4)#use profile AP7131_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write

Apply the RF Domain profile to the AP

Apply the previously created RF Domain to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the same as its associated wireless controller.

rfs4000(config-device-00-23-68-16-C6-C4)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
rfs4000(config-device-00-23-68-16-C6-C4)#Exit
rfs4000(config)#

A.1.3.5 Creating a DHCP Server Policy

A Using the Command Line Interface to Configure the WLAN

The DHCP server policy defines the parameters required to run a DHCP server on the wireless controller and assign IP addresses automatically to devices that associate. Configuring DHCP enables the reuse of a limited set of IP addresses.

To create a DHCP server policy:

rfs4000-37FABE(config)#dhcp-server-policy DHCP_POLICY_UseCase1
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#

The following table displays how IP addresses are used.

<table>
<thead>
<tr>
<th>IP Range</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.11.1 till 172.16.11.10</td>
<td>Reserved for devices that require a static IP address</td>
</tr>
<tr>
<td>172.16.11.11 till 172.16.11.200</td>
<td>Range of IP addresses that can be assigned using the DHCP server.</td>
</tr>
<tr>
<td>172.16.11.201 till 172.16.11.254</td>
<td>Reserved for devices that require a static IP address</td>
</tr>
</tbody>
</table>

In the table, the IP address range of 172.16.11.11 to 172.16.11.200 is available using the DHCP server. To configure the DHCP server:

rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#dhcp-pool DHCP_POOL_USECASE1_01
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#

Configure the address range as follows:

rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#address range 172.16.11.11 172.16.11.200
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#

Configure the IP pool used with a network segment. This starts the DHCP server on the specified interface.
Configure the RFS4000 to use the DHCP Policy

For the DHCP to work properly, the new DHCP Server Policy must be applied to the wireless controller. To apply the DHCP Server Policy to the wireless controller:

```
rfs4000-37FABE(config)#self
rfs4000-37FABE(config-device-03-14-28-57-14-28)#use dhcp-server-policy DHCP_POLICY_UseCase1
rfs4000-37FABE(config-device-03-14-28-57-14-28)#commit write
rfs4000-37FABE(config-device-03-14-28-57-14-28)#exit
```

A.1.3.6 Completing and Testing the Configuration

Using the Command Line Interface to Configure the WLAN

A wireless client must be configured to associate with the wireless controller managed WLAN. The following information must be defined:

- **SSID:** WLAN_USECASE_01
- **Country:** Same as the country configured in Creating a RF Domain on page A-3. In this scenario, the country code is set to US.
- **Mode:** Infrastructure

With the WLAN set to beacon, use the wireless client’s discovery client to discover the configured WLAN and associate.
APPENDIX B
PUBLICLY AVAILABLE SOFTWARE

B.1 General Information

This document contains information regarding licenses, acknowledgments and required copyright notices for open source packages used in the following products:

Access Points
- AP8232, AP8222, AP8163, AP8132, AP8122, AP7181, AP7161, AP7131, AP7502, AP7522, AP7532, AP7562, AP6562, AP6532, AP6522, AP6521, AP6511, AP650, AP622, AP621

Wireless Switches
- NX9600, NX9510, NX9500, NX9000, NX7500, NX7510, NX7520, NX7530, NX6524, NX6500, NX5500, NX4524, NX4500, RFS7000, RFS6000, RFS4000, RFS4011

B.2 Open Source Software Used

The following table lists the Open Source Software used, their version numbers and Web sites from where they can be downloaded:

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>URL</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Web Server</td>
<td>1.3.41</td>
<td><a href="http://www.apache.org/">http://www.apache.org/</a></td>
<td>Apache License, Version 2.0</td>
</tr>
<tr>
<td>Asterisk</td>
<td>1.2.24</td>
<td><a href="http://www.asterisk.org/">http://www.asterisk.org/</a></td>
<td>GNU General Public License 2.0</td>
</tr>
<tr>
<td>advas</td>
<td>0.2.3 ???</td>
<td><a href="http://advas.sourceforge.net/">http://advas.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>alivepdf</td>
<td>0.1.4.9</td>
<td><a href="https://code.google.com/p/alivepdf/">https://code.google.com/p/alivepdf/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>autoconf</td>
<td>2.62</td>
<td><a href="http://www.gnu.org/software/autoconf/">http://www.gnu.org/software/autoconf/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>automake</td>
<td>1.9.6</td>
<td><a href="http://www.gnu.org/software/automake/">http://www.gnu.org/software/automake/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>bash</td>
<td>4.2</td>
<td><a href="http://www.gnu.org/software/bash/">http://www.gnu.org/software/bash/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>bind</td>
<td>9.3.2</td>
<td><a href="http://www.isc.org/">http://www.isc.org/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>binutils</td>
<td>2.19.1</td>
<td><a href="http://www.gnu.org/software/binutils/">http://www.gnu.org/software/binutils/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>bison</td>
<td>2.3</td>
<td><a href="http://www.gnu.org/software/bison/">http://www.gnu.org/software/bison/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>bluez</td>
<td>5.7</td>
<td><a href="http://www.bluez.org/">http://www.bluez.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>bridge</td>
<td>1.0.4</td>
<td><a href="http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/">http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>bridge-utils</td>
<td>1.0.4</td>
<td><a href="http://sourceforge.net/projects/bridge/">http://sourceforge.net/projects/bridge/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>busybox</td>
<td>1.14.4</td>
<td><a href="http://www.busybox.net/">http://www.busybox.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>czjson</td>
<td>1.0.8</td>
<td><a href="https://pypi.python.org/pypi/czjson/1.0.8">https://pypi.python.org/pypi/czjson/1.0.8</a></td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>dhcp</td>
<td>3.0.3</td>
<td><a href="http://www.isc.org/software/dhcp">http://www.isc.org/software/dhcp</a></td>
<td>ISC License</td>
</tr>
<tr>
<td>diffutils</td>
<td>2.8.1</td>
<td><a href="http://www.gnu.org/software/diffutils/">http://www.gnu.org/software/diffutils/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>dmalloc</td>
<td>5.5.2</td>
<td><a href="http://dmalloc.com/">http://dmalloc.com/</a></td>
<td>None</td>
</tr>
<tr>
<td>dmidecode</td>
<td>2.11</td>
<td><a href="http://savannah.nongnu.org/projects/dmidecode/">http://savannah.nongnu.org/projects/dmidecode/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>dnsmasq</td>
<td>2.47</td>
<td><a href="http://www.thekelleys.org.uk/dnsmasq/doc.html">http://www.thekelleys.org.uk/dnsmasq/doc.html</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>dosfstools</td>
<td>2.11</td>
<td><a href="http://www.daniel-baumann.ch/software/dosfstools/">http://www.daniel-baumann.ch/software/dosfstools/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>dropbear</td>
<td>0.55</td>
<td><a href="http://matt.ucc.asn.au/dropbear/dropbear.html">http://matt.ucc.asn.au/dropbear/dropbear.html</a></td>
<td>DropBear License</td>
</tr>
<tr>
<td>e2fsprogs</td>
<td>1.41.12</td>
<td><a href="http://e2fsprogs.sourceforge.net/">http://e2fsprogs.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>ethtool</td>
<td>2.6.35</td>
<td><a href="http://www.kernel.org/pub/software/network/ethtool/">http://www.kernel.org/pub/software/network/ethtool/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>flashrom</td>
<td>0.9.4</td>
<td><a href="http://flashrom.org/Flashrom">http://flashrom.org/Flashrom</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>flex</td>
<td>2.5.4</td>
<td><a href="http://flex.sourceforge.net/">http://flex.sourceforge.net/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>freeipmi</td>
<td>1.0.8</td>
<td><a href="http://www.gnu.org/software/freeipmi/">http://www.gnu.org/software/freeipmi/</a></td>
<td>GNU General Public License, version 3</td>
</tr>
<tr>
<td>freeradius</td>
<td>2.0.2</td>
<td><a href="http://www.freeradius.org/">http://www.freeradius.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>glib2</td>
<td>2.30.2</td>
<td><a href="http://www.gtk.org/">http://www.gtk.org/</a></td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>hostapd</td>
<td>0.6.9</td>
<td><a href="http://hostap.epitest.fi/hostapd/">http://hostap.epitest.fi/hostapd/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>hotplug</td>
<td>1.3</td>
<td><a href="http://sourceforge.net/projects/linux-hotplug/">http://sourceforge.net/projects/linux-hotplug/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>i2ctools</td>
<td>3.0.3</td>
<td><a href="http://www.lm-sensors.org/wiki/I2CTools">http://www.lm-sensors.org/wiki/I2CTools</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>iproute2</td>
<td>050816</td>
<td><a href="http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2">http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>iptables</td>
<td>1.4.3</td>
<td><a href="http://www.netfilter.org/projects/iptables/index.html">http://www.netfilter.org/projects/iptables/index.html</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>ipxe</td>
<td>1.0.0</td>
<td><a href="http://ipxe.org/">http://ipxe.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>kerberos</td>
<td>None</td>
<td><a href="http://web.mit.edu/Kerberos/">http://web.mit.edu/Kerberos/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>libcares</td>
<td>1.7.1</td>
<td><a href="http://c-ares.haxx.se/">http://c-ares.haxx.se/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>libcurl</td>
<td>7.30.0</td>
<td><a href="http://curl.haxx.se/libcurl/">http://curl.haxx.se/libcurl/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>libdevmapper</td>
<td>2.02.66</td>
<td><a href="">ftp://sources.redhat.com/pub/lvm2/old</a></td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>libffi</td>
<td>3.0.7</td>
<td><a href="http://sourceware.org/libffi/">http://sourceware.org/libffi/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>libgcrypt</td>
<td>1.4.5</td>
<td>ftp://ftp.gnupg.org/GnuPG/libgcrypt/</td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>libgmp</td>
<td>4.2.2</td>
<td><a href="http://gmplib.org/">http://gmplib.org/</a></td>
<td>GNU Lesser General Public License, version 3.0</td>
</tr>
<tr>
<td>libgpg-error</td>
<td>1.6</td>
<td>ftp://ftp.gnupg.org/GnuPG/libgpg-error/</td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>libharu</td>
<td>2.1.0</td>
<td><a href="http://libharu.org/">http://libharu.org/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>libhttp-parser</td>
<td>None</td>
<td>None</td>
<td>MIT License</td>
</tr>
<tr>
<td>libiconv</td>
<td>1.14</td>
<td><a href="http://savannah.gnu.org/projects/libiconv/">http://savannah.gnu.org/projects/libiconv/</a></td>
<td>GNU General Public License 2.0</td>
</tr>
<tr>
<td>libjson</td>
<td>0.10</td>
<td><a href="http://sourceforge.net/projects/libjson/">http://sourceforge.net/projects/libjson/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>libkerberos</td>
<td>0.1</td>
<td><a href="http://web.mit.edu/kerberos/dist/">http://web.mit.edu/kerberos/dist/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>libncurses</td>
<td>5.4</td>
<td><a href="http://www.gnu.org/software/ncurses/">http://www.gnu.org/software/ncurses/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>libpam</td>
<td>1.1.1</td>
<td><a href="http://www.kernel.org/pub/linux/libs/pam/">http://www.kernel.org/pub/linux/libs/pam/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>libpcap</td>
<td>1.0.0</td>
<td><a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>libpcre</td>
<td>8.21</td>
<td>ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/</td>
<td>The BSD License</td>
</tr>
<tr>
<td>libpopt</td>
<td>1.14</td>
<td><a href="http://freecode.com/projects/popt">http://freecode.com/projects/popt</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>libraryopt</td>
<td>1.01</td>
<td><a href="http://sourceforge.net/projects/libraryopt/">http://sourceforge.net/projects/libraryopt/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>libreadline</td>
<td>4.3</td>
<td><a href="http://cnswww.cns.cwru.edu/php/chet/readline/rtop.html">http://cnswww.cns.cwru.edu/php/chet/readline/rtop.html</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>libtool</td>
<td>1.5.24</td>
<td><a href="http://www.gnu.org/software/libtool/">http://www.gnu.org/software/libtool/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>libusb</td>
<td>0.1.12</td>
<td><a href="http://www.libusb.org/">http://www.libusb.org/</a></td>
<td>GNU Lesser General Public License, version 2.0</td>
</tr>
<tr>
<td>libvirt</td>
<td>0.9.11</td>
<td><a href="http://libvirt.org/sources/">http://libvirt.org/sources/</a></td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>libxml2</td>
<td>2.8.0</td>
<td><a href="http://xmlsoft.org/">http://xmlsoft.org/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>libxslt</td>
<td>1.1.26</td>
<td><a href="http://xmlsoft.org/xslt/">http://xmlsoft.org/xslt/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>lighttpd</td>
<td>1.4.29</td>
<td><a href="http://www.lighttpd.net/">http://www.lighttpd.net/</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>lilo</td>
<td>22.6</td>
<td><a href="http://lilo.alioth.debian.org/">http://lilo.alioth.debian.org/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>linux</td>
<td>2.6.28.9</td>
<td><a href="http://www.kernel.org/">http://www.kernel.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>ltp</td>
<td>20060717</td>
<td><a href="https://github.com/linux-test-project/ltp">https://github.com/linux-test-project/ltp</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>lxml</td>
<td>2.3beta1</td>
<td><a href="http://lxml.de/">http://lxml.de/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>lzma</td>
<td>4.32</td>
<td><a href="http://www.7-zip.org/sdk.html">http://www.7-zip.org/sdk.html</a></td>
<td>GNU Lesser General Public License, version 2.0</td>
</tr>
<tr>
<td>lzma</td>
<td>4.57</td>
<td><a href="http://www.7-zip.org/sdk.html">http://www.7-zip.org/sdk.html</a></td>
<td>GNU Lesser General Public License, version 2.0</td>
</tr>
<tr>
<td>M2Crypto</td>
<td>0.21.1</td>
<td><a href="http://chandlerproject.org/bin/view/Projects/MeTooCrypto">http://chandlerproject.org/bin/view/Projects/MeTooCrypto</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>m4</td>
<td>1.4.5</td>
<td><a href="http://www.gnu.org/software/m4/">http://www.gnu.org/software/m4/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>madwifi</td>
<td>trunk-r3314</td>
<td><a href="http://madwifi-project.org/">http://madwifi-project.org/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>mdadm</td>
<td>3.2.2</td>
<td><a href="http://neil.brown.name/blog/mdadm">http://neil.brown.name/blog/mdadm</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>memtester</td>
<td>4.0.8</td>
<td><a href="http://pyropus.ca/software/memtester/">http://pyropus.ca/software/memtester/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>mkyaffs</td>
<td>None</td>
<td><a href="http://www.yaffs.net/">http://www.yaffs.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>mod_ssl</td>
<td>2.8.3.1-1.3.41</td>
<td><a href="http://www.modssl.org/">http://www.modssl.org/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>nano</td>
<td>1.2.4</td>
<td><a href="http://www.nano-editor.org/">http://www.nano-editor.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>no-vnc</td>
<td>None</td>
<td><a href="http://kanaka.github.io/noVNC/">http://kanaka.github.io/noVNC/</a></td>
<td>Mozilla Public License, version 2</td>
</tr>
<tr>
<td>ntp</td>
<td>4.2.6p4</td>
<td><a href="http://www.ntp.org/index.html">http://www.ntp.org/index.html</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>Open Scales</td>
<td>2.2</td>
<td><a href="http://openscales.org/">http://openscales.org/</a></td>
<td>GNU Lesser General Public License, version 3.0</td>
</tr>
<tr>
<td>OpenStreetMap</td>
<td></td>
<td><a href="http://www.openstreetmap.org/">http://www.openstreetmap.org/</a></td>
<td>Creative Commons Attribution-ShareAlike License, version 3.0</td>
</tr>
<tr>
<td>openldap</td>
<td>2.4.25</td>
<td><a href="http://www.openldap.org/foundation/">http://www.openldap.org/foundation/</a></td>
<td>The Open LDAP Public License</td>
</tr>
<tr>
<td>openllpd</td>
<td>0.0.3alpha</td>
<td><a href="http://openllpd.sourceforge.net/">http://openllpd.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>openssh</td>
<td>5.4p1</td>
<td><a href="http://www.openssh.com/">http://www.openssh.com/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>openssl</td>
<td>1.2.3</td>
<td><a href="http://www.openssl.org/">http://www.openssl.org/</a></td>
<td>OpenSSL License</td>
</tr>
<tr>
<td>openwrt</td>
<td>trunk-r15025</td>
<td><a href="http://www.openwrt.org/">http://www.openwrt.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>opkg</td>
<td>trunk-r4564</td>
<td><a href="http://code.google.com/p/opkg/">http://code.google.com/p/opkg/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>oprofile</td>
<td>0.9.2</td>
<td><a href="http://oprofile.sourceforge.net/news/">http://oprofile.sourceforge.net/news/</a></td>
<td>GNU Lesser General Public License 2.1</td>
</tr>
<tr>
<td>ProGuard</td>
<td>4.8</td>
<td><a href="http://proguard.sourceforge.net/">http://proguard.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>pciutils</td>
<td>3.1.8</td>
<td><a href="http://mj.ucw.cz/sw/pciutils/">http://mj.ucw.cz/sw/pciutils/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>pdnsd</td>
<td>1.2.5</td>
<td><a href="http://members.home.nl/p.a.rombouts/pdnsd/">http://members.home.nl/p.a.rombouts/pdnsd/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>picocom</td>
<td>1.6</td>
<td><a href="http://code.google.com/p/picocom/">http://code.google.com/p/picocom/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>ping</td>
<td>1.0</td>
<td>None</td>
<td>The BSD License</td>
</tr>
<tr>
<td>pkg-config</td>
<td>0.22</td>
<td><a href="http://pkg-config.freedesktop.org/wiki/">http://pkg-config.freedesktop.org/wiki/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>ppp</td>
<td>2.4.3</td>
<td><a href="http://ppp.samba.org/ppp/">http://ppp.samba.org/ppp/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>procrname</td>
<td>0.2</td>
<td><a href="http://code.google.com/p/procrname/">http://code.google.com/p/procrname/</a></td>
<td>GNU Lesser General Public License, version 2.0</td>
</tr>
<tr>
<td>procps</td>
<td>3.2.8</td>
<td><a href="http://procps.sourceforge.net/">http://procps.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>psmisc</td>
<td>22.8</td>
<td><a href="http://sourceforge.net/projects/psmisc/">http://sourceforge.net/projects/psmisc/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>pure-ftpd</td>
<td>1.0.22</td>
<td><a href="http://www.pureftpd.org/project/pure-ftpd">http://www.pureftpd.org/project/pure-ftpd</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>pychecker</td>
<td>0.8.18</td>
<td><a href="http://pychecker.sourceforge.net/">http://pychecker.sourceforge.net/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>pyparsing</td>
<td>1.5.1</td>
<td><a href="http://sourceforge.net/projects/pyparsing/">http://sourceforge.net/projects/pyparsing/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>pyxapi</td>
<td>0.1</td>
<td><a href="http://www.pps.jussieu.fr/%7EYlg/PyXAPI/">http://www.pps.jussieu.fr/%7EYlg/PyXAPI/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>quagga</td>
<td>0.99.16</td>
<td><a href="http://www.quagga.net">http://www.quagga.net</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>quilt</td>
<td>0.47</td>
<td><a href="http://savannah.nongnu.org/projects/quilt/">http://savannah.nongnu.org/projects/quilt/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>radius</td>
<td>2.1.12</td>
<td><a href="http://freeradius.org/">http://freeradius.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>rp-pppoe</td>
<td>3.1.0</td>
<td>[<a href="http://www.roaringpenguin.com/products/">http://www.roaringpenguin.com/products/</a> pppoe](<a href="http://www.roaringpenguin.com/products/">http://www.roaringpenguin.com/products/</a> pppoe)</td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>rsync</td>
<td>3.0.6</td>
<td><a href="http://rsync.samba.org/">http://rsync.samba.org/</a></td>
<td>GNU General Public License, version 3</td>
</tr>
<tr>
<td>samba</td>
<td>3.5.1</td>
<td><a href="http://www.samba.org">http://www.samba.org</a></td>
<td>GNU General Public License, version 3</td>
</tr>
<tr>
<td>smarttools</td>
<td>6.2</td>
<td><a href="http://smartmontools.sourceforge.net">http://smartmontools.sourceforge.net</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>snmpagent</td>
<td>5.0.9</td>
<td><a href="http://sourceforge.net/">http://sourceforge.net/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>sqlite3</td>
<td>3007900</td>
<td><a href="http://www.sqlite.org/">http://www.sqlite.org/</a></td>
<td>None</td>
</tr>
<tr>
<td>squid</td>
<td>2.7.STABLE9</td>
<td><a href="http://www.squid-cache.org/">http://www.squid-cache.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>stackless python</td>
<td>2.5.2</td>
<td><a href="http://www.stackless.com/">http://www.stackless.com/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>strace</td>
<td>4.5.20</td>
<td><a href="http://sourceforge.net/projects/strace/">http://sourceforge.net/projects/strace/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>strongswan</td>
<td>4.4.0</td>
<td><a href="http://www.strongswan.org">http://www.strongswan.org</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>tar</td>
<td>1.17</td>
<td><a href="http://www.gnu.org/software/tar/">http://www.gnu.org/software/tar/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>tcpdump</td>
<td>4.0.0</td>
<td><a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>u-boot</td>
<td>trunk-2010-03-30</td>
<td><a href="http://www.denx.de/wiki/U-Boot/">http://www.denx.de/wiki/U-Boot/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>uClibc</td>
<td>0.9.29</td>
<td><a href="http://www.uclibc.org/">http://www.uclibc.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>uClibc</td>
<td>0.9.30</td>
<td><a href="http://www.uclibc.org/">http://www.uclibc.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>uci</td>
<td>0.7.5</td>
<td><a href="http://www.openwrt.org/">http://www.openwrt.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>udev</td>
<td>147</td>
<td><a href="https://launchpad.net/udev">https://launchpad.net/udev</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>udev</td>
<td>r106</td>
<td><a href="http://www.kernel.org/pub/linux/utils/kernel/hotplug/">http://www.kernel.org/pub/linux/utils/kernel/hotplug/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>usbutils</td>
<td>0.73</td>
<td><a href="http://www.linux-usb.org/">http://www.linux-usb.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>util-linux</td>
<td>2.20</td>
<td><a href="http://www.kernel.org/pub/linux/utils/util-linux/">http://www.kernel.org/pub/linux/utils/util-linux/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>valgrind</td>
<td>3.5.0</td>
<td><a href="http://valgrind.org/">http://valgrind.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>wanpipe</td>
<td>3.5.18</td>
<td><a href="http://wiki.sangoma.com/wanpipe-linux-drivers">http://wiki.sangoma.com/wanpipe-linux-drivers</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>websocket</td>
<td>2.4</td>
<td><a href="https://github.com/nori0428/mod_websocket">https://github.com/nori0428/mod_websocket</a></td>
<td>MIT License</td>
</tr>
<tr>
<td>wget</td>
<td>1.14</td>
<td><a href="http://www.gnu.org/software/wget/">http://www.gnu.org/software/wget/</a></td>
<td>GNU General Public License, version 3</td>
</tr>
<tr>
<td>wireless_tools</td>
<td>r29</td>
<td><a href="http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html">http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>wpa_supplicant</td>
<td>2.0</td>
<td><a href="http://hostap.epitest.fi/wpa_supplicant/">http://hostap.epitest.fi/wpa_supplicant/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>wuftpd</td>
<td>1.0.21</td>
<td><a href="http://wu-ftpdr.therockgarden.ca/">http://wu-ftpdr.therockgarden.ca/</a></td>
<td>WU-FTPD Software License</td>
</tr>
<tr>
<td>XenAPI</td>
<td>None</td>
<td><a href="http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html">http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>xen</td>
<td>4.1.2</td>
<td><a href="http://www.xen.org/">http://www.xen.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>xen-crashdump-analysr</td>
<td>20130505</td>
<td><a href="http://xenbits.xen.org/people/andrewcoop/">http://xenbits.xen.org/people/andrewcoop/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>zlib</td>
<td>1.2.5</td>
<td><a href="http://www.zlib.net/">http://www.zlib.net/</a></td>
<td>zlib License</td>
</tr>
<tr>
<td>zwave</td>
<td>0.1</td>
<td><a href="http://code.google.com/p/open-zwave/">http://code.google.com/p/open-zwave/</a></td>
<td>GNU Lesser General Public License, version 2.1</td>
</tr>
</tbody>
</table>
B.3 OSS Licenses

B.3.1 Apache License, Version 2.0

Apache License
Version 2.0, January 2004
http://www.apache.org/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such
Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
   b. You must cause any modified files to carry prominent notices stating that You changed the files; and
   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
   d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.
   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.
END OF TERMS AND CONDITIONS

B.3.2 The BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B.3.3 Creative Commons Attribution-ShareAlike License, version 3.0

Creative Commons Attribution-ShareAlike 3.0 Unported

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

1. "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.
2. "Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License.

3. "Creative Commons Compatible License" means a license that is listed at http://creativecommons.org/compatiblelicenses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.

4. "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.

5. "License Elements" means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

6. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

7. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

8. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

9. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

10. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

11. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.
3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

1. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;
2. to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked “The original work was translated from English to Spanish,” or a modification could indicate “The original work has been modified.”;
3. to Distribute and Publicly Perform the Work including as incorporated in Collections; and,
4. to Distribute and Publicly Perform Adaptations

For the avoidance of doubt:
1. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;
2. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,
3. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

1. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License.

This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.

2. You may Distribute or Publicly Perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US); (iv) a Creative Commons Compatible License. If you license the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that license. If you license the Adaptation under the terms of any of the licenses mentioned in (i), (ii) or (iii) (the “Applicable License”), you must comply with the terms of the Applicable License generally and the following provisions: (I) You must include a copy of, or the URI for, the Applicable License with every copy of each Adaptation You Distribute or Publicly Perform; (II) You may not offer or impose any terms on the Adaptation that restrict the terms of the Applicable License or the ability of the recipient of the Adaptation to exercise the rights granted to that recipient under the terms of the Applicable License; (III) You must keep intact all notices that refer to the Applicable License and to the disclaimer of warranties with every copy of the ork as included in the Adaptation You Distribute or Publicly Perform; (IV) when You Distribute
or Publicly Perform the Adaptation, You may not impose any effective technological measures on the Adaptation that restrict the ability of a recipient of the Adaptation from You to exercise the rights granted to that recipient under the terms of the Applicable License. This Section 4(b) applies to the Adaptation as incorporated in a Collection, but this does not require the Collection apart from the Adaptation itself to be made subject to the terms of the Applicable License.

3. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution (“Attribution Parties”) in Licensor’s copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv), consistent with Section 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., “French translation of the Work by Original Author,” or “Screenplay based on original Work by Original Author”). The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

4. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author’s honor or reputation. Licensor agrees that in those jurisdictions (e.g., Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author’s honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

1. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

2. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election
will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

1. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

2. Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

3. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the emainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

4. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

5. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of he Licensor and You.

6. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.

Creative Commons may be contacted at http://creativecommons.org/.

B.3.4 DropBear License

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2004 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LibTomCrypt and LibTomMath are written by Tom St Denis, and are .

=====

sshpty.c is taken from OpenSSH 3.5p1,
    Copyright (c) 1995 Tatu Ylonen , Espoo, Finland
    All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

=====

loginrec.c
loginrec.h
atomicio.h
atomicio.c
and strcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

-----------------------------------------------------------------------------------------------
B.3.5 GNU General Public License, version 2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by theGNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.
When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for
the work may be a derivative work of the Library even though the source code is not. Whether this is true is
especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for
this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and
small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of
whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still
fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms
of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly
with the Library itself.

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library
to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided
that the terms permit modification of the work for the customer's own use and reverse engineering for debugging
such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its
use are covered by this License. You must supply a copy of this License. If the work during execution displays
copyright notices, you must include the copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including
whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the
work is an executable linked with the Library, with the complete machine-readable "work that uses the Library",
as object code and/or source code, so that the user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood that the user who changes the contents of definitions
files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses
at run time a copy of the library already present on the user's computer system, rather than copying library
functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs
one, as long as the modified version is interface-compatible with the version that the work was made with.

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified
in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to
copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs
needed for reproducing the executable from it. However, as a special exception, the materials to be distributed
need not include anything that is normally distributed (in either source or binary form) with the major components
(compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself
accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not
normally accompany the operating system. Such a contradiction means you cannot use both them and the Library
together in an executable that you distribute.

You may place library facilities that are a work based on the Library side-by-side in a single library together with
other library facilities not covered by this License, and distribute such a combined library, provided that the
separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and
provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other
library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and
explaining where to find the accompanying uncombined form of the same work.
You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE
ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

B.3.6 GNU Lesser General Public License 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA  02110-1301  USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL.  It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.
Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.
1. You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

2. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. The modified work must itself be a software library.
   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

5. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.
6. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being
compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the
Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library
(because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered
by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work
may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if
the work can be linked without the Library, or if the work is itself a Library. The threshold for this to be true is not precisely
defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small
inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally
a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of
Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the
Library itself.

7. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to
produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the
terms permit modification of the work for the customer’s own use and reverse engineering for debugging such
modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are
covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you
must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this
License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including
whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work
is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object
code and/or source code, so that the user can modify the Library and then relink to produce a modified executable
containing the modified Library. (It is understood that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run
time a copy of the library already present on the user’s computer system, rather than copying library functions into the
executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the
modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified
in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy
the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed
for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include
anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so
on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an
executable that you distribute.
8. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
   a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
   b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

9. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

11. Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

12. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

13. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

14. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
15. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

16. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

B.3.7 GNU General Public License, version 3

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program—to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.
For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users’ freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.
TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.


The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.
2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of echnological measures.


You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.
A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install
modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.
Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.


You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.
If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.


If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot conveying a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

B.3.8 ISC License

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

B.3.9 GNU Lesser General Public License, version 3.0

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.
The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:
   a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or
   b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.


The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:
   a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.
   b) Accompany the object code with a copy of the GNU GPL and this license document.


You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:
   a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.
   b) Accompany the Combined Work with a copy of the GNU GPL and this license document.
   c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.
   d) Do one of the following:
      0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.
      1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.
      e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

B.3.10 GNU General Public License 2.0

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.
Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, thus in effect making the program proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.
1. You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. The modified work must itself be a software library.
   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.
5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution...
of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write
to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

B.3.11 GNU Lesser General Public License, version 2.0

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.
Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered
only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   * a) The modified work must itself be a software library.
   * b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   * c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   * d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest you rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, s the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.
5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License. However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY
15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

B.3.12 GNU Lesser General Public License, version 2.1

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA  02110-1301  USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL.  It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the
original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered
only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.
   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-
readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at runtime a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so
on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an
executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other
library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution
of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these
two things:

   a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library
      facilities. This must be distributed under the terms of the Sections above.
   b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining
      where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License.
Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically
terminate your rights under this License. However, parties who have received copies, or rights, from you under this License
will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to
modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License.
Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this
License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from
the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not
impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing
compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent
issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of
this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy
simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not
distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all
those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License
would be to refrain entirely from distribution of the Library.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section
   is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity
of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system
which is implemented by public license practices. Many people have made generous contributions to the wide range of
software distributed through that system in reliance on consistent application of that system; it is up to the author/donor

to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces,
the original copyright holder who places the Library under this License may add an explicit geographical distribution
limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such
case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to
time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or
concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies
to it and "any later version", you have the option of following the terms and conditions either of that version or of any later
version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose
any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with
these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write
to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of
preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software
generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT
PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE
LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR
ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED
INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY
OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

B.3.13 MIT License

Permission is hereby granted, without written agreement and without license or royalty fees, to use, copy, modify,
and distribute this software and its documentation for any purpose, provided that the above copyright notice and
the following two paragraphs appear in all copies of this software.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT,
SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE
AND ITS DOCUMENTATION, EVEN IF THE COPYRIGHT HOLDER HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE COPYRIGHT HOLDER SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE COPYRIGHT HOLDER HAS
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

B.3.14 Mozilla Public License, version 2

Version 2.0

1. Definitions

   1.1. Contributor means each individual or legal entity that creates, contributes to the creation of, or owns
   Covered Software.
1.2. Contributor Version means the combination of the Contributions of others (if any) used by a Contributor and that particular Contribution.

1.3. Contribution means Covered Software of a particular Contributor.

1.4. Covered Software means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. Incompatible With Secondary Licenses means
   1. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or
   2. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. Executable Form means any form of the work other than Source Code Form.

1.7. Larger Work means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. License means this document.

1.9. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. Modifications means any of the following:
   1. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or
   2. any new file in Source Code Form that contains any Covered Software.

1.11. Patent Claims of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. Secondary License means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. Source Code Form means the form of the work preferred for making modifications.

1.14. You (or Your) means an individual or a legal entity exercising rights under this License. For legal entities, You includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

   Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

   1. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and
   2. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

   The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope
The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

1. for any code that a Contributor has removed from Covered Software; or
2. for infringements caused by: (i) Your and any other third party’s modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or
3. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

1. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and
2. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients’ rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms
You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation
If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty
Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability
Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party’s negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation
Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party’s ability to bring cross-claims or counter-claims.
9. Miscellaneous
This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License
10.1. New Versions
Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions
You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions
If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses
If you choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice
This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/. You may add additional accurate notices of copyright ownership.

Exhibit B - Incompatible With Secondary Licenses Notice
This Source Code Form is Incompatible With Secondary Licenses, as defined by the Mozilla Public License, v. 2.0.

B.3.15 The Open LDAP Public License

The OpenLDAP Public License
Version 2.8, 17 August 2003
Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:
1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted..

B.3.16 OpenSSL License

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org

5. Products derived from this software may not be called "OpenSSL" nor may OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

B.3.17 WU-FTPD Software License

WU-FTPD SOFTWARE LICENSE

Use, modification, or redistribution (including distribution of any modified or derived work) in any form, or on any medium, is permitted only if all the following conditions are met:

1. Redistributions qualify as "freeware" or "Open Source Software" under the following terms:

   a. Redistributions are made at no charge beyond the reasonable cost of materials and delivery. Where redistribution of this software is as part of a larger package or combined work, this restriction applies only to the
costs of materials and delivery of this software, not to any other costs associated with the larger package or combined work.

b. Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means all files included in the original distribution, including all modifications or additions, on a medium and in a form allowing fully working executable programs to be produced.

2. Redistributions of Source Code must retain the copyright notices as they appear in each Source Code file and the COPYRIGHT file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

Copyright (c) 1999,2000,2001 WU-FTPD Development Group.
All rights reserved.
The Regents of the University of California.
Portions Copyright (c) 1993, 1994 Washington University in Saint Louis.
Portions Copyright (c) 1996, 1998 Berkeley Software Design, Inc.
Portions Copyright (c) 1998 Sendmail, Inc.
Portions Copyright (c) 1989 Massachusetts Institute of Technology.
Portions Copyright (c) 1997 Stan Barber.
Portions Copyright (c) 1997 Kent Landfield.

Use and distribution of this software and its source code are governed by the terms and conditions of the WU-FTPD Software License ("LICENSE").
If you did not receive a copy of the license, it may be obtained online at http://www.wu-ftpd.org/license.html

4. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the WU-FTPD Development Group, the Washington University at Saint Louis, Berkeley Software Design, Inc., and their contributors."

5. Neither the name of the WU-FTPD Development Group, nor the names of any copyright holders, nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission. The names "wuftp" and "wu-ftpd" are trademarks of the WU-FTPD Development Group and the Washington University at Saint Louis.

6. Disclaimer/Limitation of Liability:

THIS SOFTWARE IS PROVIDED BY THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, AND CONTRIBUTORS, "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, OR CONTRIBUTORS, BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. USE, MODIFICATION, OR REDISTRIBUTION, OF THIS SOFTWARE IMPLIES ACCEPTANCE OF ALL TERMS AND CONDITIONS OF THIS LICENSE.
B.3.18 zlib License

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly        Mark Adler
jloup@gzip.org          madler@alumni.caltech.edu
jloup@gzip.org          madler@alumni.caltech.edu
C.1 Support Center

If you have a problem with your equipment, contact support for your region. Support and issue resolution is provided for products under warranty or that are covered by a services agreement. Contact information and Web self-service is available by visiting www.zebra.com/support.

When contacting support, please provide the following information:

• Serial number of the unit
• Model number or product name
• Software type and version number

Support responds to calls by email or telephone within the time limits set forth in support agreements. If you purchased your product from a business partner, contact that business partner for support.

Customer Support Web Site

The Support Web site, located at www.zebra.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Manuals

www.zebra.com/doc