## TABLE OF CONTENTS

### ABOUT THIS GUIDE

#### Chapter 1, INTRODUCTION

1.1 CLI Overview ........................................................................................................................................................... 1-2  
1.2 Getting Context Sensitive Help .................................................................................................................................. 1-7  
1.3 Using the No Command .......................................................................................................................................... 1-9  
  1.3.1 Basic Conventions ......................................................................................................................................... 1-9  
1.4 Using CLI Editing Features and Shortcuts .............................................................................................. 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 ...................................................................................................................... 1-11  
  1.4.4 Creating Profiles ........................................................................................................................................ 1-11  
  1.4.5 Change the default profile by creating vlan 150 and mapping to ge3 Physical interface ....................................................................... 1-12  
  1.4.6 Remote Administration .................................................................................................................................. 1-13  

#### Chapter 2, USER EXEC MODE COMMANDS

2.1 User Exec Commands ....................................................................................................................................... 2-3  
  2.1.1 captive-portal-page-upload .......................................................................................................... 2-5  
  2.1.2 change-passwd ............................................................................................................................................. 2-7  
  2.1.3 clear ................................................................................................................................................ 2-8  
  2.1.4 clock ................................................................................................................................................ 2-16  
  2.1.5 cluster ................................................................................................................................................ 2-17  
  2.1.6 connect ................................................................................................................................................ 2-18  
  2.1.7 create-cluster ...................................................................................................................................... 2-19  
  2.1.8 crypto ................................................................................................................................................ 2-20  
  2.1.9 device-upgrade ................................................................................................................................... 2-31  
  2.1.10 disable ............................................................................................................................................... 2-42  
  2.1.11 enable ............................................................................................................................................... 2-43  
  2.1.12 join-cluster ...................................................................................................................................... 2-44  
  2.1.13 l2tpv3 ............................................................................................................................................... 2-46
Chapter 3, PRIVILEGED EXEC MODE COMMANDS

3.1 Privileged Exec Mode Commands

3.1.1 archive ................................................................. 3-5
3.1.2 boot ............................................................... 3-7
3.1.3 captive-portal-page-upload .................................. 3-8
3.1.4 cd ..................................................................... 3-10
3.1.5 change-passwd .................................................... 3-11
3.1.6 clear ............................................................... 3-12
3.1.7 clock ............................................................... 3-22
3.1.8 cluster ............................................................. 3-23
3.1.9 configure ......................................................... 3-24
3.1.10 connect ........................................................... 3-25
3.1.11 copy ............................................................... 3-26
3.1.12 create-cluster .................................................. 3-27
3.1.13 crypto ............................................................. 3-29
3.1.14 delete ............................................................. 3-40
3.1.15 device-upgrade ................................................. 3-41
3.1.16 diff ................................................................. 3-51
3.1.17 dir ................................................................. 3-52
3.1.18 disable ............................................................ 3-53
3.1.19 edit ................................................................. 3-54
3.1.20 enable ............................................................. 3-55
3.1.21 erase .............................................................. 3-56
3.1.22 halt ................................................................. 3-57
3.1.23 join-cluster ....................................................... 3-58
3.1.24 l2tpv3 ............................................................. 3-59
3.1.25 logging ............................................................ 3-61
3.1.26 mint ............................................................... 3-62
3.1.27 mkdird ............................................................. 3-64
3.1.28 more .............................................................. 3-65
3.1.29 no ................................................................. 3-66
Chapter 5, COMMON COMMANDS

5.1 Common Commands ................................................................. 5-2
  5.1.1 clrscr ................................................................. 5-3
  5.1.2 commit ............................................................ 5-4
  5.1.3 exit ................................................................. 5-5
  5.1.4 help ................................................................. 5-6
  5.1.5 no ................................................................. 5-10
  5.1.6 revert ............................................................. 5-12
  5.1.7 service ............................................................ 5-13
  5.1.8 show ............................................................... 5-46
  5.1.9 write ............................................................... 5-48

Chapter 6, SHOW COMMANDS

6.1 show commands ................................................................. 6-2
  6.1.1 show ............................................................... 6-5
  6.1.2 adoption ......................................................... 6-11
  6.1.3 boot ............................................................... 6-14
  6.1.4 bonjour ............................................................ 6-15
  6.1.5 captive-portal .................................................. 6-16
  6.1.6 captive-portal-page-upload ................................ 6-20
  6.1.7 cdp ................................................................. 6-21
  6.1.8 clock ............................................................... 6-23
  6.1.9 cluster .............................................................. 6-24
  6.1.10 commands ...................................................... 6-25
  6.1.11 context ............................................................ 6-26
  6.1.12 critical-resources ............................................ 6-27
  6.1.13 crypto ............................................................. 6-28
  6.1.14 device-upgrade .................................................... 6-31
  6.1.15 dot1x ............................................................. 6-34
  6.1.16 environmental-sensor ....................................... 6-36
  6.1.17 event-history ................................................ 6-40
  6.1.18 event-system-policy ....................................... 6-41
  6.1.19 file ................................................................. 6-42
  6.1.20 firewall ............................................................ 6-43
  6.1.21 global ............................................................. 6-46
  6.1.22 gre ................................................................. 6-48
  6.1.23 interface .......................................................... 6-49
  6.1.24 ip ................................................................. 6-53
  6.1.25 ip-access-list ................................................... 6-59
  6.1.26 l2tpv3 ............................................................ 6-61
  6.1.27 ldap-agent ....................................................... 6-64
Chapter 7, PROFILES

7.1 Profile Config Commands

7.1.1 adopter-auto-provisioning-policy-lookup

7.1.2 adoption

7.1.3 alias

7.1.4 ap300

7.1.5 area
7.1.6 arp ......................................................................................................................................................7-20
7.1.7 auto-learn-staging-config .......................................................... .............................................................7-22
7.1.8 autogen-uniqueid .................................................................................................................................7-23
7.1.9 autoinstall ........................................................................................................................................7-25
7.1.10 bluetooth-detection .......................................................................................................................7-26
7.1.11 bridge ..........................................................................................................................................7-27
7.1.12 captive-portal ................................................................................................................................7-47
7.1.13 cdp ..................................................................................................................................................7-128
7.1.14 cluster ........................................................................................................................................7-49
7.1.15 configuration-persistence .......................................................... .........................................................7-51
7.1.16 controller ....................................................................................................................................7-52
7.1.17 critical-resource .............................................................................................................................7-55
7.1.18 crypto ..........................................................................................................................................7-58
7.1.19 device-upgrade .............................................................................................................................7-119
7.1.20 dot1x ..........................................................................................................................................7-122
7.1.21 dscp-mapping ................................................................................................................................7-124
7.1.22 email-notification ..........................................................................................................................7-125
7.1.23 enforce-version ................................................................................................................................7-127
7.1.24 environmental-sensor ....................................................................................................................7-128
7.1.25 events ..........................................................................................................................................7-130
7.1.26 export ..........................................................................................................................................7-131
7.1.27 floor ............................................................................................................................................7-132
7.1.28 gre ................................................................................................................................................7-133
7.1.29 http-analyze ...............................................................................................................................7-134
7.1.30 http-analyze (NX45XX, NX65XX, and NX9000) ..............................................................................7-145
7.1.31 interface ......................................................................................................................................7-146
7.1.32 ip ..................................................................................................................................................7-301
7.1.33 l2tpv3 ..........................................................................................................................................7-311
7.1.34 l3e-lite-table ................................................................................................................................7-313
7.1.35 led .................................................................................................................................................7-314
7.1.36 led-timeout ................................................................................................................................7-315
7.1.37 legacy-auto-downgrade .................................................................................................................7-316
7.1.38 legacy-auto-update .........................................................................................................................7-317
7.1.39 lldp ..............................................................................................................................................7-318
7.1.40 load-balancing .............................................................................................................................7-319
7.1.41 logging ......................................................................................................................................7-324
7.1.42 mac-address-table .........................................................................................................................7-326
7.1.43 mac-auth ....................................................................................................................................7-328
7.1.44 memory-profile .............................................................................................................................7-331
7.1.45 meshpoint-device ..........................................................................................................................7-332
7.1.46 meshpoint-monitor-interval .........................................................................................................7-333
7.1.47 min-misconfiguration-recovery-time ............................................................................................7-334
7.1.48 mint ................................................................................................................................................7-335
7.1.49 misconfiguration-recovery-time .................................................................................................7-341
7.1.50 neighbor-inactivity-timeout ...........................................................................................................7-342
7.1.51 neighbor-info-interval ..................................................................................................................7-343
7.1.52 no ................................................................................................................................................7-344
Chapter 8, AAA-POLICY

8.1 aaa-policy ...................................................... 8-3
8.1.1 accounting .................................................. 8-4
8.1.2 attribute ....................................................... 8-8
8.1.3 authentication ............................................. 8-11
Chapter 9, AUTO-PROVISIONING-POLICY
9.1 auto-provisioning-policy ................................................................. 9-4
  9.1.1 adopt .................................................................................... 9-5
  9.1.2 default-adopt ....................................................................... 9-11
  9.1.3 deny ..................................................................................... 9-12
  9.1.4 evaluate-always ................................................................. 9-15
  9.1.5 redirect ............................................................................... 9-16
  9.1.6 upgrade ............................................................................. 9-19
  9.1.7 no ....................................................................................... 9-22

Chapter 10, ASSOCIATION-ACL-POLICY
10.1 association-acl-policy ............................................................... 10-3
  10.1.1 deny ............................................................................... 10-4
  10.1.2 no .................................................................................... 10-6
  10.1.3 permit ............................................................................ 10-8

Chapter 11, ACCESS-LIST
11.1 ip-access-list .......................................................................... 11-3
  11.1.1 deny ............................................................................... 11-4
  11.1.2 disable ........................................................................... 11-14
  11.1.3 insert .............................................................................. 11-17
  11.1.4 no .................................................................................. 11-19
  11.1.5 permit ........................................................................... 11-21
  11.2 mac-access-list .................................................................... 11-31
  11.2.1 deny .............................................................................. 11-32
  11.2.2 disable ........................................................................... 11-35
  11.2.3 insert .............................................................................. 11-37
  11.2.4 no .................................................................................. 11-39
  11.2.5 permit ........................................................................... 11-41

Chapter 12, DHCP-SERVER-POLICY
12.1 dhcp-server-policy ................................................................. 12-3
  12.1.1 bootp .............................................................................. 12-4
  12.1.2 dhcp-class ....................................................................... 12-5
  12.1.3 dhcp-pool ........................................................................ 12-11
  12.1.4 dhcp-server ..................................................................... 12-57
  12.1.5 no ................................................................................... 12-59
Chapter 13, FIREWALL-POLICY
13.1 firewall-policy ................................................................. 13-3
  13.1.1 acl-logging ............................................................... 13-4
  13.1.2 alg ............................................................................ 13-5
  13.1.3 clamp ......................................................................... 13-6
  13.1.4 dhcp-offer-convert ................................................... 13-7
  13.1.5 dns-snoop ................................................................. 13-8
  13.1.6 firewall ..................................................................... 13-9
  13.1.7 flow ........................................................................... 13-10
  13.1.8 ip ............................................................................... 13-12
  13.1.9 ip-mac ....................................................................... 13-20
  13.1.10 logging ................................................................. 13-23
  13.1.11 no ........................................................................... 13-25
  13.1.12 proxy-arp ............................................................... 13-32
  13.1.13 stateful-packet-inspection-12 ................................. 13-33
  13.1.14 storm-control ......................................................... 13-34
  13.1.15 virtual-defragmentation ......................................... 13-36

Chapter 15, MINT-POLICY
15.1 mint-policy ................................................................. 15-2
  15.1.1 level ..................................................................... 15-3
  15.1.2 mtu ......................................................................... 15-4
  15.1.3 router ................................................................. 15-5
  15.1.4 udp ........................................................................ 15-6
  15.1.5 no ........................................................................... 15-7

Chapter 16, MANAGEMENT-POLICY
16.1 management-policy ....................................... 16-3
  16.1.1 aaa-login ............................................................... 16-4
  16.1.2 banner ................................................................. 16-6
  16.1.3 ftp .......................................................................... 16-7
  16.1.4 http ....................................................................... 16-9
  16.1.5 https ............................................................... 16-10
  16.1.6 idle-session-timeout ............................................ 16-11
  16.1.7 no ................................................................. 16-12
  16.1.8 privilege-mode-password ..................................... 16-16
  16.1.9 restrict-access ................................................. 16-17
  16.1.10 snmp-server ...................................................... 16-20
  16.1.11 ssh ................................................................. 16-25
  16.1.12 telnet ............................................................... 16-26
  16.1.13 user ................................................................. 16-27
## Chapter 17, RADIUS-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1 radius-group</td>
<td>17-2</td>
</tr>
<tr>
<td>17.1.1 guest</td>
<td>17-4</td>
</tr>
<tr>
<td>17.1.2 policy</td>
<td>17-5</td>
</tr>
<tr>
<td>17.1.3 rate-limit</td>
<td>17-9</td>
</tr>
<tr>
<td>17.1.4 no</td>
<td>17-10</td>
</tr>
<tr>
<td>17.2 radius-server-policy</td>
<td>17-13</td>
</tr>
<tr>
<td>17.2.1 authentication</td>
<td>17-15</td>
</tr>
<tr>
<td>17.2.2 chase-referral</td>
<td>17-17</td>
</tr>
<tr>
<td>17.2.3 crl-check</td>
<td>17-18</td>
</tr>
<tr>
<td>17.2.4 ldap-agent</td>
<td>17-19</td>
</tr>
<tr>
<td>17.2.5 ldap-group-verification</td>
<td>17-21</td>
</tr>
<tr>
<td>17.2.6 ldap-server</td>
<td>17-22</td>
</tr>
<tr>
<td>17.2.7 local</td>
<td>17-25</td>
</tr>
<tr>
<td>17.2.8 nas</td>
<td>17-26</td>
</tr>
<tr>
<td>17.2.9 no</td>
<td>17-27</td>
</tr>
<tr>
<td>17.2.10 proxy</td>
<td>17-31</td>
</tr>
<tr>
<td>17.2.11 session-resumption</td>
<td>17-33</td>
</tr>
<tr>
<td>17.2.12 use</td>
<td>17-34</td>
</tr>
<tr>
<td>17.3 radius-user-pool-policy</td>
<td>17-35</td>
</tr>
<tr>
<td>17.3.1 user</td>
<td>17-36</td>
</tr>
<tr>
<td>17.3.2 no</td>
<td>17-38</td>
</tr>
</tbody>
</table>

## Chapter 18, RADIO-QOS-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.1 radio-qos-policy</td>
<td>18-3</td>
</tr>
<tr>
<td>18.1.1 accelerated-multicast</td>
<td>18-4</td>
</tr>
<tr>
<td>18.1.2 admission-control</td>
<td>18-5</td>
</tr>
<tr>
<td>18.1.3 no</td>
<td>18-8</td>
</tr>
<tr>
<td>18.1.4 smart-aggregation</td>
<td>18-11</td>
</tr>
<tr>
<td>18.1.5 service</td>
<td>18-13</td>
</tr>
<tr>
<td>18.1.6 wmm</td>
<td>18-15</td>
</tr>
</tbody>
</table>

## Chapter 19, ROLE-POLICY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.1 role-policy</td>
<td>19-2</td>
</tr>
<tr>
<td>19.1.1 default-role</td>
<td>19-3</td>
</tr>
<tr>
<td>19.1.2 ldap-deadperiod</td>
<td>19-5</td>
</tr>
<tr>
<td>19.1.3 ldap-query</td>
<td>19-6</td>
</tr>
<tr>
<td>19.1.4 ldap-server</td>
<td>19-7</td>
</tr>
<tr>
<td>19.1.5 ldap-timeout</td>
<td>19-9</td>
</tr>
<tr>
<td>19.1.6 no</td>
<td>19-10</td>
</tr>
<tr>
<td>19.1.7 user-role</td>
<td>19-12</td>
</tr>
</tbody>
</table>
Chapter 20, SMART-RF-POLICY

20.1 smart-rf-policy ................................................................. 20-3
  20.1.1 area ............................................................................. 20-4
  20.1.2 assignable-power ..................................................... 20-5
  20.1.3 avoidance-time ......................................................... 20-6
  20.1.4 channel-list ................................................................. 20-7
  20.1.5 channel-width ............................................................ 20-8
  20.1.6 coverage-hole-recovery ........................................... 20-10
  20.1.7 dfs ............................................................................ 20-12
  20.1.8 enable ....................................................................... 20-13
  20.1.9 group-by ................................................................. 20-14
  20.1.10 interference-recovery ............................................. 20-15
  20.1.11 neighbor-recovery .................................................. 20-17
  20.1.12 no .......................................................................... 20-19
  20.1.13 sensitivity ............................................................... 20-21
  20.1.14 smart-ocs-monitoring ............................................ 20-22

Chapter 21, WIPS-POLICY

21.1 wips-policy ................................................................. 21-3
  21.1.1 ap-detection ............................................................ 21-4
  21.1.2 enable ..................................................................... 21-5
  21.1.3 event ........................................................................ 21-6
  21.1.4 history-throttle-duration ..................................... 21-10
  21.1.5 interference-event .................................................. 21-11
  21.1.6 no .......................................................................... 21-12
  21.1.7 signature ................................................................. 21-16
  21.1.8 use ........................................................................ 21-34

Chapter 22, WLAN-QOS-POLICY

22.1 wlan-qos-policy ............................................................. 22-2
  22.1.1 accelerated-multicast ............................................ 22-3
  22.1.2 classification .......................................................... 22-5
  22.1.3 multicast-mask ....................................................... 22-7
  22.1.4 no .......................................................................... 22-8
  22.1.5 qos .......................................................................... 22-11
  22.1.6 rate-limit ............................................................... 22-12
  22.1.7 svp-prioritization .................................................. 22-15
  22.1.8 voice-prioritization ................................................ 22-16
  22.1.9 wmm ............................................................... 22-17

Chapter 23, L2TPV3-POLICY

23.1 l2tpv3-policy-commands ............................................ 23-3
  23.1.1 cookie-size .......................................................... 23-5
  23.1.2 failover-delay .................................................... 23-6
### Chapter 24, ROUTER-MODE COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>router-mode</td>
<td>24-3</td>
</tr>
<tr>
<td>area</td>
<td>24-4</td>
</tr>
<tr>
<td>auto-cost</td>
<td>24-13</td>
</tr>
<tr>
<td>default-information</td>
<td>24-14</td>
</tr>
<tr>
<td>ip</td>
<td>24-15</td>
</tr>
<tr>
<td>network</td>
<td>24-16</td>
</tr>
<tr>
<td>ospf</td>
<td>24-17</td>
</tr>
<tr>
<td>passive</td>
<td>24-18</td>
</tr>
<tr>
<td>redistribute</td>
<td>24-19</td>
</tr>
<tr>
<td>route-limit</td>
<td>24-20</td>
</tr>
<tr>
<td>router-id</td>
<td>24-21</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>24-22</td>
</tr>
<tr>
<td>no</td>
<td>24-23</td>
</tr>
</tbody>
</table>
Chapter 29, CRYPTO-CMP-POLICY
  29.1 crypto-cmp-policy-instance .......................................................... 29-2
    29.1.1 ca-server ............................................................................. 29-3
    29.1.2 trustpoint ........................................................................... 29-4
    29.1.3 use ..................................................................................... 29-6
    29.1.4 no ..................................................................................... 29-7
  29.2 other-cmp-related-commands ..................................................... 29-8
    29.2.1 use ..................................................................................... 29-9
    29.2.2 show .................................................................................. 29-10

Chapter 30, ROAMING ASSIST POLICY
  30.1 roaming-assist-policy-instance .................................................. 30-2
    30.1.1 action ............................................................................... 30-3
    30.1.2 aggressiveness ................................................................. 30-4
    30.1.3 detection-threshold .......................................................... 30-5
    30.1.4 handoff-count ................................................................. 30-6
    30.1.5 handoff-threshold ............................................................ 30-7
    30.1.6 monitoring interval .......................................................... 30-8
    30.1.7 sampling interval ............................................................ 30-9
    30.1.8 no ................................................................................... 30-10

Appendix A, CONTROLLER MANAGED WLAN USE CASE
  A.1 Creating a First Controller Managed WLAN ................................ A-2
    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.1 General Information ................................................................. B-1
  B.2 Open Source Software Used .................................................... B-2
  B.3 OSS Licenses ........................................................................ B-11
Appendix C, CUSTOMER SUPPORT
ABOUT THIS GUIDE

This manual supports the following wireless controllers, service platforms, and access points:

- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX4500, NX6500, NX7500, NX9000, NX9500, NX9510, NX9600
- Access Points – AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP7131, AP7161, AP7181, AP7502, AP7522, AP7532, AP8122, AP8132, AP8222, AP8232

---

**NOTE:** ES6510 is an *Ethernet Switch* managed by a wireless controller or service platform, such as RFS4000, RFS6000, RFS7000, NX9000, NX9500, NX9600, NX9510. 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 and AP8132 are collectively represented as AP81XX.
- AP8222 and AP8232 are collectively represented as AP82XX.
- NX4500 and NX4524 are collectively represented as NX45XX.
- NX6500 and NX6524 are collectively represented as NX65XX.
- NX9000, NX9500, NX9510 and NX9600 are collectively represented as NX9000 series.

---

A simplified version of the WiNG operating system *user interface* (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 point of the same model.

The WE UI is supported on the following access point models with the E-SKU:

- AP6511, AP6521, AP6522, AP6562, AP7502, AP7522, and AP7532
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, NX6500, NX6524, NX7500, 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, `rfs7000-37FABE> show interface ge 1` is documented as: `show interface ge <1-4>` 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 ......` is documented as: `show [adoption|advanced-wips|ap-upgrade|......]` where:
| | • show – is the command – displays information
| | • [adoption|advanced-wips|ap-upgrade|......] – 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.
| | » show adoption ...
| | » show advanced-wips ...
| | » show ap-upgrade ... |
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|cdp|counters|crypto|
   event-history|firewall|ip|l2tpv3-stats|lldp|
   logging|mint|rtls|spanning-tree|vrrp]
```

where:

- clear – is the command
- [arp-cache|cdp|counters|crypto|event-history|firewall|ip|l2tpv3-stats|lldp|logging|mint|rtls|spanning-tree|vrrp] – indicates that fourteen keywords are available for this command. However, only one can be used at a time.

Any command/keyword-variable 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,

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

is documented as:

```
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’)
- (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>) – is the set of recursive parameters that can be used in any order.

where every recursive command is separated by a comma ‘,’.
End-User Software License Agreement

This End-User Software License Agreement ("End-User License Agreement") is between Symbol Technologies Inc. (herein "Symbol Technologies") and End-User Customer to whom Symbol Technologies’ proprietary software or Symbol Technologies Products containing embedded, pre-loaded, or installed software ("Products") is made available. This End-User License Agreement contains the terms and conditions of the license Symbol Technologies is providing to End-User Customer, and End-User Customer’s use of the Software and Documentation. By using, downloading or installing this software, you or the entity that you represent ("End-User Customer") are consenting to be bound by and are becoming a party to this End-User License Agreement.

1. DEFINITIONS

1.1. “Documentation” means product and software documentation that specifies technical and performance features and capabilities, and the user, operation and training manuals for the Software (including all physical or electronic media upon which such information is provided).

“Open Source Software” means software with either freely obtainable source code license for modification, or permission for free distribution.

“Open Source Software License” means the terms or conditions under which the Open Source Software is licensed.

“Software” (i) means proprietary software in object code format, and adaptations, translations, decompilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by Symbol Technologies; and (iii) may contain items of software owned by a third party supplier. The term “Software” does not include any third party software provided under separate license or third party software not licensable under the terms of this Agreement. To the extent, if any, that there is a separate license agreement packaged with, or provided electronically with, a particular Product that becomes effective on an act of acceptance by the end user, then that agreement supersedes this End-User License Agreement as to the end use of that particular Product.

2. GRANT OF LICENSE

2.1. If the Software licensed under this End-User License Agreement contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not this End-User License Agreement. If there is a conflict between the terms and conditions of this End-User License Agreement and the terms and conditions of the Open Source Software Licenses governing End-User Customer’s use of the Open Source Software, the terms and conditions of the license grant of the applicable Open Source Software Licenses will take precedence over the license grants in this End-User License Agreement. If requested by End-User Customer, Symbol Technologies will use commercially reasonable efforts to: (i) determine whether any Open source Software is provided under this End-User License Agreement; (ii) identify the Open Source Software and provide End-User Customer a copy of the applicable Open Source Software License (or specify where that license may be found); and, (iii) provide End-User Customer a copy of the Open Source Software source code, without charge, if it is publicly available (although distribution fees may be applicable).

3. LIMITATIONS ON USE

3.1. End-User Customer may use the Software only for End-User Customer’s internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited and will be deemed a breach of this End-User License Agreement. Without limiting the general nature of these restrictions, End-User Customer will not make the Software available for use by third parties on a “time sharing,” “application service provider,” or “service bureau” basis or for any other similar commercial rental or sharing arrangement.

3.2. End-User Customer will not, and will not allow or enable any third party to: (i) reverse engineer, disassemble, peel components, decompile, reprogram or otherwise reduce the Software or any portion to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software with other software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party, grant any sublicense or other rights in the Software or Documentation to any third party, or take any action that would
cause the Software or Documentation to be placed in the public domain; (iv) remove, or in any way alter or obscure, any copyright notice or other notice of Symbol Technologies’ proprietary rights; (v) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by any third party or on any machine except as expressly authorized by this Agreement; or (vi) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software solely by activating a machine containing the Software. End-User Customer may make one copy of Software to be used solely for archival, back-up, or disaster recovery purposes; provided that End-User Customer may not operate that copy of the Software at the same time as the original Software is being operated. End-User Customer may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

3.3. Unless otherwise authorized by Symbol Technologies in writing, End-User Customer will not, and will not enable or allow any third party to: (i) install a licensed copy of the Software on more than one unit of a Product; or (ii) copy onto or transfer Software installed in one unit of a Product onto another device.

3.4. If End-User Customer is purchasing Products that require a site license, End-User Customer must purchase a copy of the applicable Software for each site at which End-User Customer uses such Software. End-User Customer may make one additional copy for each computer owned or controlled by End-User Customer at each such site. End-User Customer may temporarily use the Software on portable or laptop computers at other sites. End-User Customer must provide a written list of all sites where End-User Customer uses or intends to use the Software.

4. TRANSFERS
4.1. End-User Customer will not transfer the Software or Documentation to any third party without Symbol Technologies’ prior written consent. Symbol Technologies’ consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this End-User License Agreement.

5. OWNERSHIP AND TITLE
5.1. Symbol Technologies, its licensors, and its suppliers retain all of their proprietary rights in any form in and to the Software and Documentation, including, but not limited to, all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation. No rights are granted to End-User Customer under this Agreement by implication, estoppel or otherwise, except for those rights which are expressly granted to End-User Customer in this End-User License Agreement. All intellectual property developed, originated, or prepared by Symbol Technologies in connection with providing the Software, Products, Documentation or related services remains vested exclusively in Symbol Technologies, and End-User Customer will not have any shared development or other intellectual property rights.

6. CONFIDENTIALITY
6.1. End-User Customer acknowledges that the Software contains valuable proprietary information and trade secrets and that unauthorized dissemination, distribution, modification, reverse engineering, disassembly or other improper use of the Software will result in irreparable harm to Symbol Technologies for which monetary damages would be inadequate. Accordingly, End-User Customer will limit access to the Software to those of its employees and agents who need to use the Software for End-User Customer’s internal business.

7. MAINTENANCE AND SUPPORT
7.1. No maintenance or support is provided under this End-User License Agreement. Maintenance or support, if available, will be provided under a separate Software maintenance and support agreement.

8. LIMITED WARRANTY AND LIMITATION OF LIABILITY
8.1. Unless otherwise specified in the applicable warranty statement, the Documentation or in any other media at the time of shipment of the Software by Symbol Technologies, and for the warranty period specified therein, for the first 120 days after initial shipment of the Software to the End-User Customer, Symbol Technologies warrants that the Software, when installed and/or used properly, will be free from reproducible defects that materially vary from its published specifications. Symbol Technologies does not warrant that End-User Customer’s use of the Software or the
Products will be uninterrupted or error-free or that the Software or the Products will meet End-User Customer’s particular requirements.

8.2. SYMBOL TECHNOLOGIES’ TOTAL LIABILITY, AND END-USER CUSTOMER’S SOLE REMEDY, FOR ANY BREACH OF THIS WARRANTY WILL BE LIMITED TO, AT SYMBOL TECHNOLOGIES’ OPTION, REPAIR OR REPLACEMENT OF THE SOFTWARE OR PAYMENT OF END-USER CUSTOMER’S ACTUAL DAMAGES UP TO THE AMOUNT PAID TO SYMBOL TECHNOLOGIES FOR THE SOFTWARE OR THE INDIVIDUAL PRODUCT IN WHICH THE SOFTWARE IS EMBEDDED OR FOR WHICH IT WAS PROVIDED. THIS WARRANTY EXTENDS ONLY TO THE FIRST END-USER CUSTOMER; SUBSEQUENT TRANSFEREES MUST ACCEPT THE SOFTWARE “AS IS” AND WITH NO WARRANTIES OF ANY KIND. SYMBOL TECHNOLOGIES DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

8.3. IN NO EVENT WILL SYMBOL TECHNOLOGIES BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF USE, TIME OR DATA, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS, OR SAVINGS, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE LIMITATIONS IN THIS PARAGRAPH WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

9. TERM AND TERMINATION

9.1. Any use of the Software, including but not limited to use on the Products, will constitute End-User Customer’s agreement to this End-User License Agreement. End-User Customer’s right to use the Software will continue for the life of the Products with which or for which the Software and Documentation have been provided by Symbol Technologies, unless End-User Customer breaches this End-User License Agreement, in which case this End-User License Agreement and End-User Customer’s right to use the Software and Documentation may be terminated immediately by Symbol Technologies. In addition, if Symbol Technologies reasonably believes that End-User Customer intends to breach this End-User License Agreement Symbol Technologies may, by notice to End-User Customer, terminate End-User Customer’s right to use the Software.

9.2. Upon termination, Symbol Technologies will be entitled to immediate injunctive relief without proving damages and, unless End-User Customer is a sovereign government entity, Symbol Technologies will have the right to repossess all copies of the Software in End-User Customer’s possession. Within thirty (30) days after termination of End-User Customer’s right to use the Software, End-User Customer must certify in writing to Symbol Technologies that all copies of such Software have been returned to Symbol Technologies or destroyed.

10. UNITED STATES GOVERNMENT LICENSING PROVISIONS

10.1. This Section applies if End-User Customer is the United States Government or a United States Government agency. End-User Customer’s use, duplication or disclosure of the Software and Documentation under Symbol Technologies’ copyrights or trade secret rights 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 they are being provided to the Department of Defense. If the Software and Documentation are being provided to the Department of Defense, End-User Customer’s use, duplication, or disclosure of the Software and Documentation 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. The Software and Documentation may or may not include a Restricted Rights notice, or other notice referring to this End-User License Agreement. The provisions of this End-User License Agreement will continue to apply, but only to the extent that they are consistent with the rights provided to the End-User Customer under the provisions of the FAR and DFARS mentioned above, as applicable to the particular procuring agency and procurement transaction.

11. GENERAL

11.1. Copyright Notices. The existence of a copyright notice on the Software will not be construed as an admission or presumption that public disclosure of the Software or any trade secrets associated with the Software has occurred.

11.2. Compliance with Laws. End-User Customer acknowledges that the Software is subject to the laws and regulations of the United States and End-User Customer will comply with all applicable laws and regulations, including export
laws and regulations of the United States. End-User Customer will not, without the prior authorization of Symbol Technologies 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 is a material breach of this Agreement.

11.3. Third Party Beneficiaries. This End-User License Agreement is entered into solely for the benefit of Symbol Technologies and End-User Customer. No third party has the right to make any claim or assert any right under this Agreement, and no third party is deemed a beneficiary of this End-User License Agreement. Notwithstanding the foregoing, any licensor or supplier of third party software included in the Software will be a direct and intended third party beneficiary of this End-User License Agreement.

11.4. Waiver. No waiver of a right or remedy of a Party will constitute a waiver of another right or remedy of that Party.

11.5. Assignments. Symbol Technologies may assign any of its rights or sub-contract any of its obligations under this End-User License Agreement or encumber or sell any of its rights in any Software, without prior notice to or consent of End-User Customer.

11.6. Causes of Action. End-User Customer must bring any action under this End-User License Agreement within one year after the cause of action arises except that warranty claims must be brought within the applicable warranty period.

11.7. Entire Agreement and Amendment. This End-User License Agreement contains the parties’ entire agreement regarding End-User Customer’s use of the Software and may be amended only in a writing signed by both parties, except that Symbol Technologies may modify this End-User License Agreement as necessary to comply with applicable laws and regulations.

11.8. Governing Law. This End-User License Agreement is governed by the laws of the the State of Delaware in the United States to the extent that they apply and otherwise by the internal substantive laws of the country to which the Software 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.

11.9. Dispute Resolution. Unless End-User Customer is a sovereign governmental entity, any dispute arising from or in connection with this End-User License Agreement shall be submitted to the sole and exclusive forum of the state and federal courts sitting in New Castle County, Delaware (the "Delaware Courts"), and each Party irrevocably submits to the jurisdiction of the Delaware Courts for the litigation of such disputes. Each Party hereby irrevocably waives, and agrees not to assert in any suit, action or proceeding brought in the Delaware Courts, any claim or defense that the Party is not subject to the jurisdiction of the Delaware Courts, that the Delaware Courts are an inconvenient forum, or that the Delaware Courts are an improper venue.
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>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits Per Second</td>
<td>19200</td>
</tr>
<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.

1.1 CLI Overview

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.

![Figure 1-1 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)#
```

**Table 1.1** 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>ap7502</td>
</tr>
<tr>
<td>clock</td>
<td>cd</td>
<td>ap7522</td>
</tr>
<tr>
<td>cluster</td>
<td>change-passwd</td>
<td>ap7532</td>
</tr>
<tr>
<td>commit</td>
<td>clear</td>
<td>alias</td>
</tr>
<tr>
<td>connect</td>
<td>clock</td>
<td>ap300</td>
</tr>
<tr>
<td>create-cluster</td>
<td>cluster</td>
<td>ap621</td>
</tr>
<tr>
<td>crypto</td>
<td>commit</td>
<td>ap622</td>
</tr>
<tr>
<td>debug</td>
<td>configure</td>
<td>ap650</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>connect</td>
<td>ap6511</td>
</tr>
<tr>
<td>disable</td>
<td>copy</td>
<td>ap6521</td>
</tr>
<tr>
<td><strong>User Exec Mode</strong></td>
<td><strong>Priv Exec Mode</strong></td>
<td><strong>Global Configuration Mode</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>enable</td>
<td>create-cluster</td>
<td>ap6522</td>
</tr>
<tr>
<td>help</td>
<td>crypto</td>
<td>ap6532</td>
</tr>
<tr>
<td>join-cluster</td>
<td>debug</td>
<td>ap6562</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>delete</td>
<td>ap71xx</td>
</tr>
<tr>
<td>logging</td>
<td>device-upgrade</td>
<td>ap81xx</td>
</tr>
<tr>
<td>mint</td>
<td>diff</td>
<td>ap82xx</td>
</tr>
<tr>
<td>no</td>
<td>dir</td>
<td>association-acl-policy</td>
</tr>
<tr>
<td>page</td>
<td>disable</td>
<td>auto-provisioning-policy</td>
</tr>
<tr>
<td>ping</td>
<td>edit</td>
<td>captive-portal</td>
</tr>
<tr>
<td>revert</td>
<td>enable</td>
<td>bonjour-gw-discovery-policy (RFS7000 and AP7131)</td>
</tr>
<tr>
<td>service</td>
<td>erase</td>
<td>bonjour-gw-forwarding-policy (RFS7000 and AP7131)</td>
</tr>
<tr>
<td>show</td>
<td>halt</td>
<td>clear</td>
</tr>
<tr>
<td>ssh</td>
<td>help</td>
<td>client-identity</td>
</tr>
<tr>
<td>telnet</td>
<td>join-cluster</td>
<td>client-identity-group</td>
</tr>
<tr>
<td>terminal</td>
<td>l2tpv3</td>
<td>clone</td>
</tr>
<tr>
<td>time-it</td>
<td>logging</td>
<td>customize</td>
</tr>
<tr>
<td>traceroute</td>
<td>mint</td>
<td>device</td>
</tr>
<tr>
<td>watch</td>
<td>mkdir</td>
<td>device-categorization</td>
</tr>
<tr>
<td>write</td>
<td>more</td>
<td>dhcp-server-policy</td>
</tr>
<tr>
<td>clrscr</td>
<td>no</td>
<td>dns-whitelist</td>
</tr>
<tr>
<td>exit</td>
<td>page</td>
<td>event-system-policy</td>
</tr>
<tr>
<td>smart-cache (NX45XX and NX65XX)</td>
<td>ping</td>
<td>firewall-policy</td>
</tr>
<tr>
<td>virtual-machine (NX45XX, NX65XX, NX9500, NX9600 and NX9510)</td>
<td>pwd</td>
<td>global-association-list</td>
</tr>
<tr>
<td>re-elect</td>
<td></td>
<td>help</td>
</tr>
<tr>
<td>reload</td>
<td></td>
<td>host</td>
</tr>
<tr>
<td>remote-debug</td>
<td></td>
<td>igmp-snoop-policy</td>
</tr>
<tr>
<td>rename</td>
<td></td>
<td>inline-password-encryption</td>
</tr>
<tr>
<td>revert</td>
<td></td>
<td>ip</td>
</tr>
</tbody>
</table>
### 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>rmdir</td>
<td>l2tpv3</td>
<td></td>
</tr>
<tr>
<td>self</td>
<td>mac</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>management-policy</td>
<td></td>
</tr>
<tr>
<td>show</td>
<td>meshpoint</td>
<td></td>
</tr>
<tr>
<td>ssh</td>
<td>meshpoint-qos-policy</td>
<td></td>
</tr>
<tr>
<td>telnet</td>
<td>mint-policy</td>
<td></td>
</tr>
<tr>
<td>terminal</td>
<td>nac-list</td>
<td></td>
</tr>
<tr>
<td>time-it</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>traceroute</td>
<td>passpoint-policy</td>
<td></td>
</tr>
<tr>
<td>upgrade</td>
<td>password-encryption</td>
<td></td>
</tr>
<tr>
<td>upgrade-abort</td>
<td>profile</td>
<td></td>
</tr>
<tr>
<td>watch</td>
<td>radio-qos-policy</td>
<td></td>
</tr>
<tr>
<td>clrscr</td>
<td>radius-group</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>radius-server-policy</td>
<td></td>
</tr>
<tr>
<td>smart-cache</td>
<td>radius-user-pool-policy</td>
<td></td>
</tr>
<tr>
<td>virtual-machine</td>
<td>rename</td>
<td></td>
</tr>
<tr>
<td>raid</td>
<td>rf-domain</td>
<td></td>
</tr>
<tr>
<td>nx45xx series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nx65xx series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nx75xx series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nx9000 series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>role-policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>routing-policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>self</td>
<td></td>
<td></td>
</tr>
<tr>
<td>smart-rf-policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wips-policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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>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>
<tr>
<td></td>
<td></td>
<td>smart-cache-policy (NX45XX and NX65XX)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>url-list (NX45XX and NX65XX)</td>
</tr>
</tbody>
</table>
1.2 Getting Context Sensitive Help

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&lt;Tab&gt;</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 ?

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 ?
ap300                          Set global AP300 parameters
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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force-send-config</td>
<td>Resend configuration to the device</td>
</tr>
<tr>
<td>force-update-vm-stats</td>
<td>Force VM statistics to be pushed up to the NOC</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Wireless load-balancing service commands</td>
</tr>
<tr>
<td>locator</td>
<td>Enable leds flashing on the device</td>
</tr>
<tr>
<td>mint</td>
<td>MiNT protocol</td>
</tr>
<tr>
<td>pktcap</td>
<td>Start packet capture</td>
</tr>
<tr>
<td>pm</td>
<td>Process Monitor</td>
</tr>
<tr>
<td>radio</td>
<td>Radio parameters</td>
</tr>
<tr>
<td>radius</td>
<td>Radius test</td>
</tr>
<tr>
<td>request-full-config-from-adopter</td>
<td>Request full configuration from the adopter</td>
</tr>
<tr>
<td>set</td>
<td>Set validation mode</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>signal</td>
<td>Send a signal to a process</td>
</tr>
<tr>
<td>smart-rf</td>
<td>Smart-RF Management Commands</td>
</tr>
<tr>
<td>ssm</td>
<td>Command related to ssm</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>syslog</td>
<td>Test the syslog server configuration</td>
</tr>
<tr>
<td>trace</td>
<td>Trace a process for system calls and signals</td>
</tr>
<tr>
<td>wireless</td>
<td>Command related to wireless</td>
</tr>
</tbody>
</table>

rfs7000-37FABE#

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. Back up 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?').
1.3 Using the No Command

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

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

Table 1.2 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. In Table 1.2, bold characters indicate the relation between a letter and its function.

<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 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>or Ctrl-B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right Arrow</td>
<td>Forward character</td>
<td>Moves the cursor one character to the right</td>
</tr>
<tr>
<td>or Ctrl-F</td>
<td></td>
<td></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>
<tr>
<td>Ctrl-K</td>
<td></td>
<td>Deletes from the cursor to end of the line</td>
</tr>
<tr>
<td>Ctrl-P</td>
<td></td>
<td>Obtains the prior command from memory</td>
</tr>
<tr>
<td>Ctrl-N</td>
<td></td>
<td>Obtains the next command from memory</td>
</tr>
<tr>
<td>Esc-C</td>
<td></td>
<td>Converts the letter at the cursor to uppercase</td>
</tr>
<tr>
<td>Esc-L</td>
<td></td>
<td>Converts the letter at the cursor to lowercase</td>
</tr>
<tr>
<td>Esc-D</td>
<td></td>
<td>Deletes the remainder of a word</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td></td>
<td>Deletes the word up to the cursor</td>
</tr>
<tr>
<td>Ctrl-Z</td>
<td></td>
<td>Returns to the root prompt</td>
</tr>
<tr>
<td>Ctrl-T</td>
<td></td>
<td>Transposes the character to the left of the cursor with the character located at the cursor</td>
</tr>
<tr>
<td>Ctrl-L</td>
<td></td>
<td>Clears the screen</td>
</tr>
</tbody>
</table>
1.4.2 Completing a Partial Command Name

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#co?
  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

rfs7000-37FABE#
```

**NOTE:** The characters entered before the question mark are reprinted to the screen to complete the command entry.

1.4.3 Command Output pagination

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.

1.4.4 Creating Profiles

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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510
- a default profile for each of the following access points:
  - AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
To modify the default profile to assign an IP address to the management port:

```plaintext
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
rfs7000-37FABE(config)#
```

The following command displays a default AP71XX profile:

```plaintext
rfs7000-37FABE(config)#profile ap71xx 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---

**1.4.5 Change the default profile by creating vlan 150 and mapping to ge3 Physical interface**

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

```plaintext
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
```
1.4.5.1 Viewing Configured APs

To view previously configured APs, enter the following command:

```
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>ap7131-4AA708</td>
<td>00-04-96-4A-A7-08</td>
<td>default-ap71xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</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>3</td>
<td>ap650-000001</td>
<td>00-A0-F8-00-00-01</td>
<td>default-ap650</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

```
rfs7000-37FABE(config)#
```

1.4.6 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 to use SSH for remote administration tasks.

1.4.6.1 Configuring Telnet for Management Access

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).

```
rfs7000-37FABE> en
rfs7000-37FABE# configure terminal
```

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

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

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

```
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>admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</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 example role helpdesk access all
```

```
rfs7000-37FABE(config-management-policy-default)# commit
rfs7000-37FABE(config-management-policy-default)#show context
management-policy default
telnet
```
1. Logon to the Telnet console and provide the user details configured in the previous step to access the controller.

rfs7000 release  5.5.6.0-006D
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs7000-37FABE>

1.4.6.2 Configuring SSH

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>admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</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 5.5.6.0-006D
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
  device-upgrade              Device firmware upgrade
  disable                     Turn off privileged mode command
  enable                      Turn on privileged mode command
  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
  page                        Toggle paging
  ping                        Send ICMP 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
  time-it                     Check how long a particular command took between request and completion of response
  traceroute                 Trace route to destination
  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
<DEVICE>>


2.1 User Exec Commands

Table 2.1 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 2-7</td>
</tr>
<tr>
<td>clear</td>
<td>Resets the last saved command</td>
<td>page 2-8</td>
</tr>
<tr>
<td>clock</td>
<td>Configures the system clock</td>
<td>page 2-16</td>
</tr>
<tr>
<td>cluster</td>
<td>Accesses the cluster context</td>
<td>page 2-17</td>
</tr>
<tr>
<td>connect</td>
<td>Establishes a console connection to a remote device</td>
<td>page 2-18</td>
</tr>
<tr>
<td>create-cluster</td>
<td>Creates a new cluster on a specified device</td>
<td>page 2-19</td>
</tr>
<tr>
<td>crypto</td>
<td>Enables encryption</td>
<td>page 2-20</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings</td>
<td>page 2-31</td>
</tr>
<tr>
<td>disable</td>
<td>Turns off (disables) the privileged mode command set</td>
<td>page 2-42</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on (enables) the privileged mode command set</td>
<td>page 2-43</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 2-44</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Establishes or brings down Layer 2 Tunneling Protocol Version 3 (L2TPV3) tunnels</td>
<td>page 2-46</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging facilities</td>
<td>page 2-48</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol</td>
<td>page 2-50</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 2-52</td>
</tr>
<tr>
<td>page</td>
<td>Toggles a device’s (access point, wireless controller, or service platform) paging function</td>
<td>page 2-56</td>
</tr>
<tr>
<td>ping</td>
<td>Sends ICMP echo messages to a user-specified location</td>
<td>page 2-57</td>
</tr>
<tr>
<td>ssh</td>
<td>Opens an SSH connection between two network devices</td>
<td>page 2-58</td>
</tr>
<tr>
<td>telnet</td>
<td>Opens a Telnet session</td>
<td>page 2-59</td>
</tr>
<tr>
<td>terminal</td>
<td>Sets the length and width of the terminal window</td>
<td>page 2-60</td>
</tr>
<tr>
<td>time-it</td>
<td>Verifies the time taken by a particular command between request and response</td>
<td>page 2-61</td>
</tr>
<tr>
<td>traceroute</td>
<td>Traces the route to its defined destination</td>
<td>page 2-62</td>
</tr>
<tr>
<td>watch</td>
<td>Repeats a specific CLI command at a periodic interval</td>
<td>page 2-63</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>smart-cache</td>
<td>Pre-fetches content cache from the specified list of URLs. This command is specific to NX45XX and NX65XX series service platforms.</td>
<td>page 2-65</td>
</tr>
<tr>
<td>virtual-machine</td>
<td>Installs, configures, and monitors the status of virtual machines (VMs). This command is specific to the NX45XX, NX65XX, NX9500 and NX9510 series service platforms.</td>
<td>page 2-66</td>
</tr>
</tbody>
</table>
### 2.1.1 captive-portal-page-upload

**User Exec Commands**

Uploads captive portal advanced pages

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```plaintext
captive-portal-page-upload [<CAPTIVE-PORTAL-NAME>|cancel-upload|load-file]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME]|all|rf-domain]
  {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 load-file <CAPTIVE-PORTAL-NAME> <URL>
```

**Parameters**

- **<CAPTIVE-PORTAL-NAME>**
  - Specify the captive portal’s name (should be existing and configured).
- **<MAC/HOSTNAME>**
  - Specify AP’s MAC address or hostname.
- **all**
  - Uploads to all APs
- **upload-time <TIME>**
  - Optional. Configures an AP upload time
  - **<TIME>** — Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.
- **<DOMAIN-NAME>**
  - Uploads to APs within a specified RF Domain. Specify the RF Domain name.
- **all**
  - Uploads to APs across all RF Domains
- **from-controller**
  - Optional. Uploads to APs from the adopted device

<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;CAPTIVE-PORTAL-NAME&gt;</td>
<td>• &lt;CAPTIVE-PORTAL-NAME&gt; — Specify the captive portal’s name (should be existing and configured).</td>
</tr>
<tr>
<td>&lt;MAC/HOSTNAME&gt;</td>
<td>Uploads to a specified AP</td>
</tr>
<tr>
<td>• &lt;MAC/HOSTNAME&gt; — Specify AP’s MAC address or hostname.</td>
<td></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>
<tr>
<td>• &lt;TIME&gt; — Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
<td></td>
</tr>
<tr>
<td>rf-domain [&lt;DOMAIN-NAME]</td>
<td>all]</td>
</tr>
<tr>
<td>• &lt;DOMAIN-NAME&gt; — Uploads to APs within a specified RF Domain. Specify the RF Domain name.</td>
<td></td>
</tr>
<tr>
<td>• all — Uploads to APs across all RF Domains</td>
<td></td>
</tr>
<tr>
<td>from-controller</td>
<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.

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

captive-portal-page-upload cancel-upload
Cancels a scheduled AP 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

• captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
captive-portal-page-upload load-file
Loads captive-portal advanced pages

<CAPTIVE-PORTAL-NAME> <URL>
Specify the captive portal’s name and location. The captive portal should be existing and configured.
• <URL> – Specifies file location in the following format:
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

Examples
rfs4000-229D58>captive-portal-page-upload test1 00-04-96-4A-A7-08 upload-time 03/01/2014-12:30

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-22-9D-58</td>
<td>Fail</td>
<td>Failed to initiate page upload</td>
</tr>
</tbody>
</table>

rfs4000-229D58>
rfs4000-229D58>captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-22-9D-58</td>
<td>Success</td>
<td>Cancelled upgrade of 1 APs</td>
</tr>
</tbody>
</table>

rfs4000-229D58>
### 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

NOTE: Refer to the interface details below when using clear

- ge <index> – RFS4000 supports 5 GEs, RFS6000 supports 8 GEs, NX45XX and NX65XX series support 24 GEs
- me1 – Available in both RFS7000 and RFS6000
- up1 – Uplink interface on RFS4000

Syntax

```
clear [arp-cache|cdp|counters|crypto|event-history|gre|ip|lldp|mac-address-table|
mint|role|rtls|smart-cache|spanning-tree|vrrp]
clear arp-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>} {<1-3>}|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 [dhcp|ospf]
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {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] {on <DEVICE-NAME>}{on <DEVICE-OR-DOMAIN-NAME>}
clear spanning-tree detected-protocols {interface|on}
clear spanning-tree detected-protocols {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface [{<INTERFACE-NAME>|ge <1-5>|me1|
port-channel <1-3>|pppo1|up1|vlan <1-4094>|wwan1}] {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**

- clear arp-cache {on <DEVICE-NAME>}
  
  **arp-cache** Clears Address Resolution Protocol (ARP) cache entries on a AP, wireless controller, or service platform. This protocol matches the layer 3 IP addresses to the 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 [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>}{<1-3}>|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.

  **radio** Clears radio interface counters on a specified device or on all devices
  
  - <MAC/DEVICE-NAME> – Optional. Specify the device's hostname or MAC address.
    
    Optionally, append the radio interface number (to the radio ID) using one of the following formats: AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX (where RX is the interface number).
    
    - <1-3> – Optional. Identifies the radio interface by its index. Specify the radio interface index, if not specified as part of the radio ID.
  
  **Note:** If no device name or MAC address is specified, all radio interface counters are cleared.

  **wireless-client <MAC>** Clears counters for all wireless clients or a specified wireless client
  
  - <MAC> – Optional. Specify the wireless client's MAC address.
  
  **Note:** If no MAC address is specified, all wireless client counters are cleared.

  **on <DEVICE-OR-DOMAIN-NAME>** This keyword is common to all of the above keywords.
  
  - on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP, radio, or wireless client counters on a specified AP, wireless controller, service platform, or RF Domain.

- clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
  
  **crypto** Clears encryption module database
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **ike sa [<IP>|all]** | clears **Internet Key Exchange (IKE) security associations** (SAs)  
|   | - `<IP>` – clears IKE SA entries for the peer identified by the `<IP>` keyword  
|   | - all – clears IKE SA entries 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** {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 gre stats** {on <DEVICE-NAME>} | clears GRE tunnel statistics  
|   | - `<DEVICE-NAME>` – optional. GRE tunnel statistics on a specified device  
|   | - `<DEVICE-NAME>` – specify the name of the AP, wireless controller, or service platform.  
| **clear event-history** | clears event history cache entries  
| **clear ip dhcp bindings [ <IP>|all ]** {on <DEVICE-NAME>} | clears **Dynamic Host Configuration Protocol (DHCP)** server's IP address binding entries  
|   | - `<DEVICE-NAME>` specify the IP address to clear binding entries.  
|   | - `<DEVICE-NAME>` – specify the name of the AP, wireless controller, or service platform.  
| **clear ip ospf process** {on <DEVICE-NAME>} | clears **Open Shortest Path First (OSPF)** process and restarts the process  
|   | - `<DEVICE-NAME>` – specify the name of the AP, wireless controller, or service platform.  

**Open Shortest Path First (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.
### clear mac-address-table

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`clear mac-address-table {address &lt;MAC&gt;</td>
<td>vlan &lt;1-4094&gt;} {on &lt;DEVICE-NAME&gt;}`</td>
</tr>
</tbody>
</table>

**mac-address-table**

- **address <MAC>**
  - Specifies 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>**
  - Specifies the VLAN ID from 1 - 4094

- **on <DEVICE-NAME>**
  - Specifies the name of the AP, wireless controller, or service platform.

**Note:** 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`clear mac-address-table interface [&lt;IF-NAME&gt;</td>
<td>ge &lt;1-X&gt;</td>
</tr>
</tbody>
</table>

**mac-address-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)

- **ge <1-X>**
  - clears MAC address forwarding table for the specified GigabitEthernet interface

- **port-channel <1-X>**
  - clears MAC address forwarding table for the specified port-channel interface

- **t1e1 <1-4> <1-1>**
  - clears MAC address forwarding table for the specified T1E1L interface

- **up <1-X>**
  - clears MAC address forwarding table for the WAN Ethernet interface

**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.

**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.

**Note:** The T1E1 interfaces are supported only on the NX45XX and NX65XX series service platforms.

**Note:** 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.

**Note:** 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.

**Note:** 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>}
Clears MiNT related information

### mint
Clears MiNT related information

### mlcp history
Clears MiNT Link Creation Protocol (MLCP) client history

### 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>}
Clears LDAP server statistics

### role ldap-stats
Clears LDAP server statistics

### 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] {<DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}}
Clears Real Time Location Service (RTLS) statistics

### rtls
Clears Real Time Location Service (RTLS) statistics

### aeroscout
Clears RTLS Aeroscout statistics

### ekahau
Clears RTLS Ekahau statistics

### on <DEVICE-NAME>
This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.
- on `<DEVICE-NAME>` – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, or service platform.

### on <DEVICE-OR-DOMAIN-NAME>
This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.
- on `<DEVICE-OR-DOMAIN-NAME>` – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, service platform, or RF Domain.

### clear spanning-tree detected-protocols {on <DEVICE-NAME>}
Clears spanning tree entries on an interface, and restarts protocol migration

### 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.
### USER EXEC MODE COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear spanning-tree detected-protocols</strong> {interface [&lt;INTERFACE-NAME&gt;</td>
<td>ge &lt;1-5&gt;</td>
</tr>
<tr>
<td><strong>interface</strong> [&lt;INTERFACE-NAME&gt;</td>
<td>ge &lt;1-5&gt;</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong></td>
<td>Optional. Clears spanning tree entries on a specified device.</td>
</tr>
<tr>
<td><strong>clear vrrp</strong> [error-stats</td>
<td>stats] {on &lt;DEVICE-NAME&gt;}}</td>
</tr>
<tr>
<td><strong>vrrp</strong></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><strong>error-stats</strong></td>
<td>Clears global error statistics.</td>
</tr>
<tr>
<td><strong>stats</strong></td>
<td>Clears VRRP related statistics.</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong></td>
<td>This following keywords are common to the ‘error-stats’ and ‘stats’ parameters:</td>
</tr>
<tr>
<td><strong>clear smart-cache storage</strong> [all</td>
<td>url-regex &lt;WORD&gt;] {on &lt;DEVICE-NAME&gt;}}</td>
</tr>
<tr>
<td><strong>smart-cache storage</strong></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><strong>on &lt;DEVICE-NAME&gt;</strong></td>
<td>Optional. Clears VRRP statistics on a specified device.</td>
</tr>
</tbody>
</table>
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. \w+\.(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 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 5.5.6.0-006D
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>

rfs4000-229D58> show cdp neighbors
-----------------------------------------------
<table>
<thead>
<tr>
<th>Device ID</th>
<th>Platform</th>
<th>Local Interface</th>
<th>Port ID</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs4000-880DA7</td>
<td>RFS-4011-11110-US</td>
<td>ge1</td>
<td>ge1</td>
<td>full</td>
</tr>
<tr>
<td>rfs7000-37FDF2</td>
<td>RFS-7010-1000-WR</td>
<td>ge1</td>
<td>ge1</td>
<td>full</td>
</tr>
<tr>
<td>rfs6000-434CAA</td>
<td>RFS6000</td>
<td>ge1</td>
<td>ge1</td>
<td>full</td>
</tr>
<tr>
<td>ap7131-139B34</td>
<td>AP7131N</td>
<td>ge1</td>
<td>ge1</td>
<td>full</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

rfs4000-229D58> clear cdp neighbors
rfs4000-229D58> show cdp neighbors
rfs4000-229D58>

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-8B-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-8B-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

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**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>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">HH:MM:SS</a></td>
<td>Sets the current time (in military format hours, minutes, and seconds)</td>
</tr>
<tr>
<td>&lt;1-31&gt;</td>
<td>Sets the numerical day of the month</td>
</tr>
<tr>
<td>&lt;MONTH&gt;</td>
<td>Sets the month of the year (Jan to Dec)</td>
</tr>
<tr>
<td>&lt;1993-2035&gt;</td>
<td>Sets a valid four digit year from 1993 - 2035</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Sets the clock 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**

rfs4000-229D58>clock set 14:25:35 15 Feb 2014

rfs4000-229D58>show clock
2014-02-15 14:25:40 UTC
rfs4000-229D58>
## 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

### Syntax

```
cluster start-election
```

### Parameters

- `start-election`

| start-election | Starts a new cluster master 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 the specified device</td>
</tr>
<tr>
<td><code>join-cluster</code></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** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

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

**Parameters**

- `mint-id <MINT-ID>`
  - Connects to the remote system using its MiNT ID
  - `<MINT-ID>` — Specify the remote device’s MiNT ID.

- `<REMOTE-DEVICE-NAME>`
  - Connects to the remote system using its name
  - `<REMOTE-DEVICE-NAME>` — Specify the remote device’s name.

**Examples**

```
rfs7000-37FABE>show mint lsp-db
2 LSPs in LSP-db of 70.37.FA.BE:
LSP 68.11.E6.C4 at level 1, hostname "ap7131-11E6C4", 1 adjacencies, seqnumtr
LSP 70.37.FA.BE at level 1, hostname "rfs7000-37FABE", 1 adjacencies, seqnum20
rfs7000-37FABE>connect mint-id 68.11.E6.C4 ?
```

Entering character mode

```
rfs7000-37FABE>connect mint-id 68.11.E6.C4
```

Entering character mode

```
rfs4000-229D58>show mint lsp-db
1 LSPs in LSP-db of 68.22.9D.58:
LSP 68.22.9D.58 at level 1, hostname "rfs4000-229D58", 0 adjacencies, seqnum 606
rfs4000-229D58>connect mint-id 68.22.9D.58
```

Entering character mode

```
rfs4000-229D58>connect mint-id 68.22.9D.58
```

Entering character mode

```
rfs4000-229D58>connect mint-id 68.22.9D.58
```

Entering character mode

```
rfs4000-229D58>connect mint-id 68.22.9D.58
```

Entering character mode

```
rfs4000-229D58>connect mint-id 68.22.9D.58
```


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 balance 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

Syntax
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>create-cluster</td>
<td>Creates a cluster</td>
</tr>
<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][2]</td>
<td>Optional. Configures the cluster’s routing level</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE>create-cluster name Cluster1 ip 172.16.10.1 level 1
... creating cluster
... committing the changes
... saving the changes
[OK]
rfs7000-37FABE>
nx6500-31FABE>create-cluster <CLUSTER-NAME>

Related Commands
- cluster | Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.
- join-cluster | Adds a device, as a member, to an existing cluster of devices
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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```plaintext
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 <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase <KEY-PASSPHRASE> {background <DEVICE-NAME}>|on <DEVICE-NAME>)}
crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {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 <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {passphrase <KEY-PASSPHRASE> {background <DEVICE-NAME}>|on <DEVICE-NAME>)}
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force <DEVICE-NAME>}
crypto pki [authenticate|export|generate|import|zeroize]
crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL> {background <DEVICE-NAME}>|on <DEVICE-NAME>}
crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|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|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-subject-name <EXPORT-TO-URL> {background <DEVICE-NAME>}
crypto pki export request [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 <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] <WORD> 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>} | on <DEVICE-NAME>}
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background {on <DEVICE-NAME>} | on <DEVICE-NAME> | passphrase <KEY-PASSPHRASE> {on <DEVICE-NAME>}}
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}}
on <DEVICE-NAME>

Parameters
• crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background {on <DEVICE-NAME>} | 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>export rsa &lt;RSA-KEYPAIR-NAME&gt;</td>
<td>Exports an existing RSA Keypair to a specified destination</td>
</tr>
</tbody>
</table>
  • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. |
| <EXPORT-TO-URL> | Specify the RSA Keypair destination address in the following format: |
  • tftp://<hostname|IP>[:port]/path/file |
  • ftp://<user>:<passwd>@<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 |
| background {on <DEVICE-NAME>} | Optional. Performs export operation in the background. Optionally specify the device to perform export on. |
| on <DEVICE-NAME> | Optional. Performs export operation on a specific device. |
  • on <DEVICE-NAME> – Optional. Performs export operation on a specific device |
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

• crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>} | 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>export rsa</td>
<td>Exports a RSA Keypair to a specified destination</td>
</tr>
</tbody>
</table>
  • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. |
crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>}

Generate a new RSA Keypair

- `<RSA-KEYPAIR-NAME>` - Specify the RSA Keypair name.
- `<1024-2048>` - Sets the size of the RSA key in bits from 1024 - 2048. The default size is 1024.

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 key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background {on <DEVICE-NAME>}}

Import a RSA Keypair from a specified source

- `<RSA-KEYPAIR-NAME>` - Specify the RSA Keypair name.
- `<IMPORT-FROM-URL>` - Specify the RSA Keypair source address in the following format:
  - tftp://<hostname|IP>::<port>/path/file
  - ftp://<user>:<passwd>@<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

on <DEVICE-NAME>

Optional. Performs import operation on a specified device

- `<DEVICE-NAME>` - Specify the name of the AP, wireless controller, or service platform.

background

Optional. Performs import operation in the background

- `<DEVICE-NAME>` - Optional. Performs import operation 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> \{passphrase <KEY-PASSPHRASE> \{background \{on <DEVICE-NAME>\}|on <DEVICE-NAME>\}\}

**key** Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.

**import rsa**<RSA-KEYPAIR-NAME>

Decrypts and imports a RSA Keypair from a specified source

- <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.

**<IMPORT-FROM-URL> \{passphrase <KEY-PASSPHRASE>\}**

Specify the RSA Keypair source address in the following format:

- tftp://<hostname|IP>[:port]/path/file
- ftp://<user>:<passwd>@<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

- passphrase – Optional. Decrypts the RSA Keypair before importing
- <KEY-PASSPHRASE> – Specify the passphrase to decrypt the RSA Keypair.

**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 key zeroize <RSA-KEYPAIR-NAME> \{force \{on <DEVICE-NAME>\}|on <DEVICE-NAME>\}

**key** Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.

**zeroize rsa**<RSA-KEYPAIR-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 \{on <DEVICE-NAME>\}** 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>** 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>\}|on <DEVICE-NAME>\}

**pki** 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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki export request</td>
<td>Exports CSR to the CA for digital identity certificate. The CSR contains applicant’s details and RSA Keypair’s public key.</td>
</tr>
<tr>
<td>{generate-rsa-key</td>
<td>use-rsa-key} &lt;RSA-KEYPAIR-NAME&gt;</td>
</tr>
<tr>
<td>background {on &lt;DEVICE-NAME&gt;}</td>
<td>Optional. Performs authentication in the background. Optionally specify a device on which to perform authentication.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Performs authentication on a specified device</td>
</tr>
<tr>
<td>{email &lt;SEND-TO-EMAIL&gt;}</td>
<td>Exports CSR to a specified e-mail address</td>
</tr>
<tr>
<td>{autogen-subject-name</td>
<td>Auto generates subject name from configuration parameters. The subject name identifies the certificate.</td>
</tr>
<tr>
<td>{&lt;URL&gt;}</td>
<td>Specify CA’s location in the following format:</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>http://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>cf:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb&lt;n&gt;:/path/file</td>
</tr>
</tbody>
</table>

**Note:** The CSR is exported to the specified location.

**Note:** The CA certificate is imported from the specified location.

**Note:** The CSR is exported to the specified location.

**Note:** The CA certificate is imported from the specified location.

**Note:** The CSR is exported to the specified location.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>` | Exports CSR to the CA for a digital identity certificate.

- **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.

- **subject-name <COMMON-NAME>** | Specifies subject name to identify the certificate
- **<COMMON-NAME>** – Sets 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 in the following format:
- `tftp://<hostname|IP>[:port]/path/file`
- `ftp://<user>:<passwd>@<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`

**Note:** The CSR is exported to the specified location.

- **background** – Optional. Performs export operation in the background
- **on <DEVICE-NAME>** – Optional. Performs export operation on a specific device

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

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

- **fqdn <FQDN>** | Exports CSR to a specified Fully Qualified Domain Name (FQDN)
- `<FQDN>` – Specify the CA's FQDN.

- **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.

- **generate-rsa-key|use-rsa-key** | Generates a new RSA Keypair or uses an existing RSA Keypair

- **<FQDN>** – Specify the CA's FQDN.

- **<IP>** – Specify the CA's IP address.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL>` | Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key.
| `ip address <IP>` | Exports CSR to a specified device or system.
| `fqdn <FQDN>` | Exports CSR to a specified FQDN.
| `pki` | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
| `generate` | Generates a CA certificate and a trustpoint.
| `self-signed` | Generates a self-signed CA certificate and a trustpoint.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Specify a name for the certificate and its trustpoint.</td>
</tr>
<tr>
<td><code>&lt;EXPORT-TO-URL&gt;</code></td>
<td>Specify the destination address in the following format: tftp://&lt;hostname</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><code>&lt;KEY-PASSPHRASE&gt;</code></td>
<td>Encrypts the key with a passphrase before exporting.</td>
</tr>
<tr>
<td><code>&lt;EMAIL&gt;</code></td>
<td>Specify the email address for the certificate.</td>
</tr>
<tr>
<td><code>&lt;FQDN&gt;</code></td>
<td>Specify the CA's FQDN.</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Specify the CA's IP address.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| [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 the subject name from the configuration parameters. The subject name helps to identify the certificate. |
| email <SEND-TO-EMAIL> | Optional. Exports CSR to a specified e-mail address.  
  - <SEND-TO-EMAIL> – Specify the CA's e-mail address. |
| fqdn <FQDN> | Optional. Exports CSR to a specified FQDN.  
  - <FQDN> – Specify the CA's FQDN. |
| ip-address <IP> | Optional. Exports CSR to a specified device or system.  
  - <IP> – Specify the CA's IP address. |
| on <DEVICE-NAME> | Optional. Exports the CSR on a specified device.  
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |

- `crypto pki generate self-signed <TRUSTPOINT-NAME>` generates a self-signed CA certificate and a trustpoint.  
  - <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 CA certificates. |

- `generate self-signed <TRUSTPOINT-NAME>` generates a self-signed CA certificate and a trustpoint.  
  - <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint. |

- `[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. |

- `subject-name <COMMON-NAME>` specifies a subject name 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. |

- `<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 CSR to a specified e-mail address.  
  - <SEND-TO-EMAIL> – Specify the CA's e-mail address.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto pki import</code></td>
<td>Imports certificates, Certificate Revocation List (CRL), or a trustpoint to the selected device</td>
</tr>
<tr>
<td>`crypto pki import [certificate</td>
<td>crl] &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt;`</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Specify the trustpoint name (should be authenticated).</td>
</tr>
<tr>
<td><code>&lt;IMPORT-FROM-URL&gt;</code></td>
<td>Specify the signed server certificate or CRL source address in the following format:</td>
</tr>
<tr>
<td></td>
<td>- tftp://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>- ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>- sftp://&lt;user&gt;@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>- http://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>- cf:/path/file</td>
</tr>
<tr>
<td></td>
<td>- usb&lt;n&gt;:/path/file</td>
</tr>
<tr>
<td><code>background {on &lt;DEVICE-NAME&gt;}</code></td>
<td>Optional. Performs import operation in the background</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>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>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>
<tr>
<td><code>crypto pki import trustpoint &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt;</code></td>
<td>Imports a trustpoint and its associated CA certificate, server certificate, and private key</td>
</tr>
<tr>
<td><code>background {on &lt;DEVICE-NAME&gt;}</code></td>
<td>Specify the trustpoint name (should be authenticated).</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>

**fqdn <FQDN>**
- Optional. Exports the CSR to a specified FQDN
- **<FQDN>** – Specify the CA’s FQDN.

**ip address <IP>**
- Optional. Exports the CSR to a specified device or system
- **<IP>** – Specify the CA’s IP address.

**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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki zeroize trustpoint</td>
<td>Deletes a trustpoint and its associated CA certificate, server certificate, and private key</td>
</tr>
<tr>
<td>&lt;TRUSTPOINT-NAME&gt;</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</td>
</tr>
<tr>
<td>{on &lt;DEVICE-NAME&gt;}</td>
<td>&lt;DEVICE-NAME&gt; – Optional. Deletes private key on a specific 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></td>
<td>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>
<tr>
<td></td>
<td>Enables PKI management. Use this command to authenticate, export, generate, or delete a</td>
</tr>
<tr>
<td>pki</td>
<td>trustpoint and its associated CA certificates.</td>
</tr>
<tr>
<td></td>
<td>Optional. Performs import operation in the background</td>
</tr>
<tr>
<td></td>
<td>&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>
<tr>
<td></td>
<td>&lt;KEY-PASSPHRASE&gt; – Specify a passphrase.</td>
</tr>
<tr>
<td></td>
<td>background – Optional. Imports the encrypted trustpoint in the background</td>
</tr>
<tr>
<td></td>
<td>&lt;DEVICE-NAME&gt; – Optional. Imports the encrypted 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>

**Examples**

```
import-from-url Specify the trustpoint source address in the following format:
- tftp://<hostname|IP>:<port>/path/file
- ftp://<user>:<passwd>@<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
```

```
<IMPORT-FROM-URL> Specify the trustpoint source address in the following format:
```
rfso00-37FABE>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
rfso00-37FABE>

rfso00-37FABE>crypto pki authenticate word url background
Import of CA certificate started in background
rfso00-37FABE>

rfso00-37FABE>crypto pki import trustpoint word url passphrase word
Import operation started in background
rfso00-37FABE>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes server certificates, trustpoints and their associated certificates</td>
</tr>
</tbody>
</table>
2.1.9 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.

**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.

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 completed, the following two scenarios are possible:

   **Scenario 1:** If the upgrade/reboot options ARE NOT specified by the network administrator, the NOC controller:
   
a. Pushes the AP6562 image on to the RF Domain manager.
   
b. Reboots the active controller within the RF Domain.
   
c. 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:

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, NX7500, NX9000, NX9XXX (NX9500 and NX9510)
- Site controller – RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX7500, NX9000, or NX9XXX

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** — AP300, 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, NX9000, NX9500, NX9510

**Syntax**

```
device-upgrade  [<MAC/HOSTNAME>|all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71XX|ap7502|ap7522|ap7532|ap81XX|ap82XX|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000|cancel-upgrade|load-image|rf-domain]
```

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

```
device-upgrade  all  {\(no-reboot\)|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|ap81XX|ap82XX|rfs4000|rfs6000|rfs7000|nx45XX|nx65XX|nx75XX|nx9000]  all  {\(no-reboot\)|reboot-time <TIME>\}|upgrade-time <TIME>\}  {\(no-reboot\)|reboot-time <TIME>\}} {\(staggered-reboot\)}
```
### USER EXEC MODE COMMANDS

**device-upgrade cancel-upgrade**

- `<MAC/HOSTNAME>`
- `all`
- `ap621` | `ap622` | `ap650` | `ap6511` | `ap6521` | `ap6532` | `ap6562` | `ap71xx` | `ap7502` | `ap7522` | `ap7532` | `ap81xx` | `ap82xx` | `rfs4000` | `rfs6000` | `rfs7000` | `nx45XX` | `nx65XX` | `nx75xx` | `nx9000` | `on`

**device-upgrade cancel-upgrade**

- `<MAC/HOSTNAME>`

**device-upgrade load-image**

- `<MAC/HOSTNAME>`
- `ap621` | `ap622` | `ap650` | `ap6511` | `ap6521` | `ap6532` | `ap6562` | `ap71xx` | `ap7502` | `ap7522` | `ap7532` | `ap81xx` | `ap82xx` | `rfs4000` | `rfs6000` | `rfs7000` | `nx45XX` | `nx65XX` | `nx75xx` | `nx9000` | `<IMAGE-URL>`

**device-upgrade rf-domain**

- `<RF-DOMAIN-NAME>`
- `all`
- `ap621` | `ap622` | `ap650` | `ap6511` | `ap6521` | `ap6532` | `ap6562` | `ap71xx` | `ap7502` | `ap7522` | `ap7532` | `ap81xx` | `ap82xx` | `rfs4000` | `rfs6000` | `rfs7000` | `nx45XX` | `nx65XX` | `nx75xx` | `nx9000` | `<MAC/HOSTNAME>` | `no-reboot` | `from-controller` | `reboot-time <TIME>` | `{<MAC/HOSTNAME> | <TIME> | no-reboot | from-controller}`

**device-upgrade rf-domain**

- `<RF-DOMAIN-NAME>`
- `all`
- `ap621` | `ap622` | `ap650` | `ap6511` | `ap6521` | `ap6532` | `ap6562` | `ap71xx` | `ap7502` | `ap7522` | `ap7532` | `ap81xx` | `ap82xx` | `rfs4000` | `rfs6000` | `rfs7000` | `nx45XX` | `nx65XX` | `nx75xx` | `nx9000` | `<MAC/HOSTNAME>` | `no-reboot` | `reboot-time <TIME>` | `{<MAC/HOSTNAME> }{<MAC/HOSTNAME> | no-reboot | from-controller}`

**device-upgrade rf-domain**

- `<RF-DOMAIN-NAME>`
- `all`
- `ap621` | `ap622` | `ap650` | `ap6511` | `ap6521` | `ap6532` | `ap6562` | `ap71xx` | `ap7502` | `ap7522` | `ap7532` | `ap81xx` | `ap82xx` | `rfs4000` | `rfs6000` | `rfs7000` | `nx45XX` | `nx65XX` | `nx75xx` | `nx9000` | `<MAC/HOSTNAME>` | `no-reboot` | `reboot-time <TIME>` | `{<MAC/HOSTNAME> }{<MAC/HOSTNAME> | no-reboot | from-controller}`

**Parameters**

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

- **device-upgrade `<MAC/HOSTNAME>`**
  - `ap621` | `ap622` | `ap650` | `ap6511` | `ap6521` | `ap6532` | `ap6562` | `ap71xx` | `ap7502` | `ap7522` | `ap7532` | `ap81xx` | `ap82xx` | `rfs4000` | `rfs6000` | `rfs7000` | `nx45XX` | `nx65XX` | `nx75xx` | `nx9000` | `<MAC/HOSTNAME>` | `no-reboot` | `reboot-time <TIME>` | `{<MAC/HOSTNAME> }{<MAC/HOSTNAME> | no-reboot | from-controller}`

<table>
<thead>
<tr>
<th><code>&lt;MAC/HOSTNAME&gt;</code></th>
<th><code>Parameters</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAC/HOSTNAME&gt;</code></td>
<td>upgrades firmware on the device identified by the <code>&lt;MAC/HOSTNAME&gt;</code> keyword</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</td>
</tr>
<tr>
<td>upgrade-time <code>&lt;TIME&gt;</code></td>
<td>optional. schedules an automatic firmware upgrade</td>
</tr>
<tr>
<td>all</td>
<td>upgrades firmware on all devices</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</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 &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic reboot after a successful upgrade</td>
</tr>
<tr>
<td></td>
<td>• &lt;TIME&gt; – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>upgrade-time &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic device firmware upgrade on all devices</td>
</tr>
<tr>
<td></td>
<td>• &lt;TIME&gt; – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td></td>
<td>The following actions can be performed after a scheduled upgrade:</td>
</tr>
<tr>
<td></td>
<td>• no-reboot – Optional. Disables automatic reboot after a successful upgrade</td>
</tr>
<tr>
<td></td>
<td>(the device must be manually restarted)</td>
</tr>
<tr>
<td></td>
<td>• reboot-time &lt;TIME&gt; – 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>staggered-reboot</td>
<td>This keyword is common to all of the above.</td>
</tr>
<tr>
<td></td>
<td>• Optional. Enables staggered reboot (one at a time), without network impact</td>
</tr>
</tbody>
</table>

After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 &lt;br&gt;• <code>&lt;TIME&gt;</code> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM format.</td>
</tr>
<tr>
<td>upgrade-time <code>&lt;TIME&gt;</code></td>
<td>Optional. Schedules an automatic firmware upgrade on all devices of the specified type &lt;br&gt;• <code>&lt;TIME&gt;</code> – 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 common to all of the above. &lt;br&gt;• Optional. Enables staggered reboot (one at a time), without network impact</td>
</tr>
<tr>
<td></td>
<td>• device-upgrade cancel-upgrade [&lt;MAC/HOSTNAME&gt;</td>
</tr>
<tr>
<td>cancel-upgrade [-&lt;MAC/HOSTNAME&gt;</td>
<td>all]</td>
</tr>
</tbody>
</table>
|                        | • device-upgrade cancel-upgrade [ap621|ap622|ap650|ap651|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] all | Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. <br>• AP621 all – Cancels scheduled upgrade on all AP621s <br>• AP622 all – Cancels scheduled upgrade on all AP622s <br>• AP650 all – Cancels scheduled upgrade on all AP650s <br>• AP6511 all – Cancels scheduled upgrade on all AP6511s <br>• AP6521 all – Cancels scheduled upgrade on all AP6521s <br>• AP6522 all – Cancels scheduled upgrade on all AP6522s <br>• AP6532 all – Cancels scheduled upgrade on all AP6532s <br>• AP6562 all – Cancels scheduled upgrade on all AP6562s <br>• AP71XX all – Cancels scheduled upgrade on all AP71XXs <br>• AP7502 all – Cancels scheduled upgrade on all AP7502s <br>• AP7522 all – Cancels scheduled upgrade on all AP7522s <br>• AP7532 all – Cancels scheduled upgrade on all AP7532s <br>• AP81XX all – Cancels scheduled upgrade on all AP81XXs <br>• AP82XX all – Cancels scheduled upgrade on all AP82XXs <br>• RFS4000 all – Cancels scheduled upgrade on all RFS4000s <br>• RFS6000 all – Cancels scheduled upgrade on all RFS6000s Contd..
### device-upgrade cancel-upgrade on rf-domain [<RF-DOMAIN-NAME>|all]

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

Cancels scheduled firmware upgrade in a specified RF Domain or all RF Domains
- **<RF-DOMAIN-NAME>** – Cancels scheduled device upgrade in a specified RF Domain. Specify the RF Domain name.
- **all** – Cancels scheduled device upgrades across all RF Domains

### device-upgrade load-image [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] <IMAGE-URL>

**load-image [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] <IMAGE-URL>**

Loads device firmware image from a specified location. Select the device type and provide the location of the required device firmware image.
- **AP621 <IMAGE-URL>** – Loads AP621 firmware image
- **AP622 <IMAGE-URL>** – Loads AP622 firmware image
- **AP650 <IMAGE-URL>** – Loads AP650 firmware image
- **AP6511 <IMAGE-URL>** – Loads AP6511 firmware image
- **AP6521 <IMAGE-URL>** – Loads AP6521 firmware image
- **AP6522 <IMAGE-URL>** – Loads AP6522 firmware image
- **AP6532 <IMAGE-URL>** – Loads AP6532 firmware image
- **AP6562 <IMAGE-URL>** – Loads AP6562 firmware image
- **AP71XX <IMAGE-URL>** – Loads AP71XX firmware image
- **AP7502 <IMAGE-URL>** – Loads AP7502 firmware image
- **AP7522 <IMAGE-URL>** – Loads AP7522 firmware image
- **AP7532 <IMAGE-URL>** – Loads AP7532 firmware image
- **AP81XX <IMAGE-URL>** – Loads AP81XX firmware image
- **AP82XX <IMAGE-URL>** – Loads AP82XX firmware image
- **RFS4000 <IMAGE-URL>** – Loads RFS4000 firmware image
- **RFS6000 <IMAGE-URL>** – Loads RFS6000 firmware image
- **RFS7000 <IMAGE-URL>** – Loads RFS7000 firmware image
- **NX45XX <IMAGE-URL>** – Loads NX45XX series service platform firmware image
- **NX65XX <IMAGE-URL>** – Loads NX65XX series service platform firmware image
- **NX75XX <IMAGE-URL>** – Loads NX75XX series service platform firmware image
- **NX9000 <IMAGE-URL>** – Loads NX9000 series service platform firmware image
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>device-upgrade rf-domain</code></td>
<td>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.</td>
</tr>
<tr>
<td>`[&lt;RF-DOMAIN-NAME&gt;</td>
<td>all]`</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Upgrades devices across all RF Domains</td>
</tr>
<tr>
<td><code>&lt;MAC/HOSTNAME&gt;</code></td>
<td>Optional. Upgrades firmware on the device identified by the <code>&lt;MAC/HOSTNAME&gt;</code> keyword</td>
</tr>
</tbody>
</table>

Specify the device’s firmware image location in one of the following formats:
- `tftp://hostname|IP|[:port]/path/file`
- `ftp://user:<password>@hostname|IP|[:port]/path/file`
- `sftp://user:<password>@hostname|IP|[:port]/path/file`
- `http://hostname|IP|[:port]/path/file`
- `cf:/path/file`
- `usb<n>:/path/file`

### Examples

#### Device Upgrade

- **RF Domain:**
  - `<RF-DOMAIN-NAME>`: Specify the RF Domain name.
  - `all`: Upgrades devices across all RF Domains

- **Device Types:**
  - `<all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap75xx|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000>`

- **Optional:**
  - `<MAC/HOSTNAME>`: Specify the device’s MAC address or hostname.

- **Reboot Time:**
  - `reboot-time <TIME>`: Specifies the reboot time.

- **No-Reboot:**
  - `no-reboot`: Disables the reboot process after upgrading firmware.

- **Staggered Reboot:**
  - `(staggered-reboot)`: Enables staggered reboot for specific devices within a domain.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-reboot</td>
<td>Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)</td>
</tr>
<tr>
<td>{staggered-reboot}</td>
<td></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>{staggered-reboot}</td>
<td></td>
</tr>
<tr>
<td>staggered-reboot</td>
<td>This keyword is common to all of the above. Optional. Enables staggered reboot (one at a time), without network impact</td>
</tr>
<tr>
<td>device-upgrade rf-domain</td>
<td>Upgrades firmware on devices in a specified RF Domain or all RF Domains</td>
</tr>
<tr>
<td>`[&lt;RF-DOMAIN-NAME&gt;</td>
<td>all]`</td>
</tr>
<tr>
<td>all</td>
<td>Upgrades devices in a specified RF Domain. Specify the RF Domain name.</td>
</tr>
<tr>
<td>&lt;RF-DOMAIN-NAME&gt;</td>
<td>Upgrades devices in a specified RF Domain. Specify the RF Domain name.</td>
</tr>
<tr>
<td>all</td>
<td>Upgrades devices across all RF Domains</td>
</tr>
<tr>
<td>from-controller</td>
<td>Optional. Upgrades a device through the adopted device</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>{staggered-reboot}</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reboot-time &lt;TIME&gt;</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>{staggered-reboot}</td>
<td></td>
</tr>
<tr>
<td>upgrade-time &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic firmware upgrade</td>
</tr>
<tr>
<td>{no-reboot</td>
<td>reboot-time &lt;TIME&gt;}</td>
</tr>
<tr>
<td>staggered-reboot</td>
<td>This keyword is common to all of the above.</td>
</tr>
<tr>
<td></td>
<td>Optional. Enables staggered reboot (one at a time), without network impact</td>
</tr>
<tr>
<td>device-upgrade rf-domain</td>
<td>Upgrades firmware on devices in a specified RF Domain or all RF Domains</td>
</tr>
<tr>
<td>[&lt;RF-DOMAIN-NAME&gt;]</td>
<td>all]</td>
</tr>
<tr>
<td></td>
<td>• &lt;RF-DOMAIN-NAME&gt; – Upgrades devices in a specified RF Domain. Specify the RF Domain name.</td>
</tr>
<tr>
<td></td>
<td>• all – Upgrades devices across all RF Domains</td>
</tr>
<tr>
<td></td>
<td>After specifying the RF Domain, select the device type.</td>
</tr>
<tr>
<td></td>
<td>• all – Upgrades firmware on all devices</td>
</tr>
<tr>
<td></td>
<td>• AP621 – Upgrades firmware on all AP621s</td>
</tr>
<tr>
<td></td>
<td>• AP622 – Upgrades firmware on all AP622s</td>
</tr>
<tr>
<td></td>
<td>• AP650 – Upgrades firmware on all AP650s</td>
</tr>
<tr>
<td></td>
<td>• AP6511 – Upgrades firmware on all AP6511s</td>
</tr>
<tr>
<td></td>
<td>• AP6521 – Upgrades firmware on all AP6521s</td>
</tr>
<tr>
<td></td>
<td>• AP6522 – Upgrades firmware on all AP6522s</td>
</tr>
<tr>
<td></td>
<td>• AP71XX – Upgrades firmware on all AP71XXs</td>
</tr>
<tr>
<td></td>
<td>• AP7502 – Upgrades firmware on all AP7502s</td>
</tr>
<tr>
<td></td>
<td>• AP7522 – Upgrades firmware on all AP7522s</td>
</tr>
<tr>
<td></td>
<td>• AP7532 – Upgrades firmware on all AP7532s</td>
</tr>
<tr>
<td></td>
<td>• AP81XX – Upgrades firmware on all AP81XXs</td>
</tr>
<tr>
<td></td>
<td>• AP82XX – Upgrades firmware on all AP82XXs</td>
</tr>
<tr>
<td></td>
<td>• RFS4000 – Upgrades firmware on all RFS4000s</td>
</tr>
<tr>
<td></td>
<td>• RFS6000 – Upgrades firmware on all RFS6000s</td>
</tr>
<tr>
<td></td>
<td>• RFS7000 – Upgrades firmware on all RFS7000s</td>
</tr>
<tr>
<td></td>
<td>• NX45XX – Upgrades firmware on all NX45XX series service platforms</td>
</tr>
<tr>
<td></td>
<td>• NX65XX – Upgrades firmware on all NX65XX series service platforms</td>
</tr>
<tr>
<td></td>
<td>• NX75XX – Upgrades firmware on all NX75XX series service platforms</td>
</tr>
<tr>
<td></td>
<td>• NX9000 – Upgrades firmware on all NX9000 series service platforms</td>
</tr>
</tbody>
</table>
upgrade <TIME> | Optional. Schedules an automatic device firmware upgrade  
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
| * <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.  
|  
| 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  

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>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>NX9XXX</td>
<td>-</td>
</tr>
</tbody>
</table>

NOTE: The NX7500 series service platform supports HM networks. At the lower end, it replaces RFS7000, and at the upper end it is adopted by NX9500. A NX7500 adopted by a NX9500 is the common deployment pattern used for the NX7500 series service platform.

Examples

```
rfs4000-229D58>device-upgrade rfs4000-229D58 no-reboot  
rfs4000-229D58>  
rfs4000-229D58>show device-upgrade ?
  history History of Device Upgrade  
  load-image-status Status of firmware file download on the device  
  status Status of Device Upgrade  
  versions Versions of device-upgrade images
  
rfs4000-229D58>  
rfs4000-229D58>show device-upgrade history

---------------------------------------------------------------------  
<table>
<thead>
<tr>
<th>Device</th>
<th>RESULT</th>
<th>TIME</th>
<th>RETRIES</th>
<th>UPGRADED-BY LAST-UPDATE-ERROR</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap71xx-0F43D8</td>
<td>failed 2014-01-05 00:21:08</td>
<td>3</td>
<td>00-23-68-22-9D-58</td>
<td>Update error: Unable to get update file, failure in ftp.openssl.tar</td>
</tr>
<tr>
<td>ap6532-986C50</td>
<td>failed 2014-01-05 00:26:31</td>
<td>3</td>
<td>00-23-68-22-9D-58</td>
<td>Update error: Bad file, failure in tar. tar: invalid tar magic</td>
</tr>
</tbody>
</table>
| Total number of entries displayed: 2  
rfs4000-229D58>  
```
rfs4000-229D58> show device-upgrade versions

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>DEVICE-TYPE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs4000-229D58</td>
<td>ap621</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap622</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap650</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6511</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6521</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6522</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6532</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6562</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap71xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap81xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap82xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>rfs4000</td>
<td>none</td>
</tr>
</tbody>
</table>

rfs4000-229D58>
2.1.10 disable

User Exec Commands

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 — AP300, 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, NX9000, NX9600, NX9510

Syntax

disable

Parameters

None

Examples

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

User Exec 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 — AP300, AP621, 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, NX9000, NX9500, NX9600, NX9510

Syntax

enable

Parameters

None

Examples

rfs7000-37FABE>enable
rfs7000-37FABE#
2.1.12 \textit{join-cluster}

\textbf{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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

\textbf{Syntax}

\texttt{join-cluster <IP> user <USERNAME> password <WORD> \{level\|mode\}}

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

\textbf{Parameters}

- \texttt{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>\texttt{&lt;IP&gt;}</td>
<td>Specify the cluster member's IP address.</td>
</tr>
<tr>
<td>\texttt{user &lt;USERNAME&gt;}</td>
<td>Specify a user account with super user privileges on the new cluster member</td>
</tr>
<tr>
<td>\texttt{password &lt;WORD&gt;}</td>
<td>Specify password for the account specified in the user parameter</td>
</tr>
<tr>
<td>\texttt{level [1|2]}</td>
<td>Optional. Configures the routing level</td>
</tr>
<tr>
<td>\texttt{mode {active|standby}}</td>
<td>Optional. Configures the cluster mode</td>
</tr>
</tbody>
</table>

\textbf{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.

\textbf{Examples}

```
rfs7000-37FABE#join-cluster 172.16.10.10 user admin password example
Joining cluster at 172.16.10.10... Done
Please execute “write memory” to save cluster configuration.
```

```
rfs7000-37FABE#
```

```
nx6500-31FABE#join-cluster 172.16.10.10 user admin password example
Joining cluster at 172.16.10.10... Done
Please execute “write memory” to save cluster configuration.
```

```
nx6500-31FABE#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cluster</code></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><code>create-cluster</code></td>
<td>Creates a new cluster on a specified device</td>
</tr>
</tbody>
</table>
2.1.13 l2tpv3

**User Exec Commands**

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

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**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
  - `<DEVICE-NAME>`: Optional. Specifies 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>`: Specifies the tunnel name.
  - `<SESSION-NAME>`: Specifies the session name.
  - `down`: Brings down the specified session
  - `up`: Establishes the specified session
  - `<DEVICE-NAME>`: Optional. Specifies 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
  - `<DEVICE-NAME>`: Optional. Specifies the name of the AP, wireless controller, or service platform.
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 23, L2TPV3-POLICY.*
2.1.14 logging

User Exec Commands

Modifies message logging settings

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

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>monitor</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>&lt;0-7&gt;</td>
<td>Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:</td>
</tr>
<tr>
<td>alerts</td>
<td>Immediate action needed (severity=1)</td>
</tr>
<tr>
<td>critical</td>
<td>Critical conditions (severity=2)</td>
</tr>
<tr>
<td>debugging</td>
<td>Debugging messages (severity=7)</td>
</tr>
<tr>
<td>emergencies</td>
<td>System is unusable (severity=0)</td>
</tr>
<tr>
<td>errors</td>
<td>Error conditions (severity=3)</td>
</tr>
<tr>
<td>informational</td>
<td>Informational messages (severity=6)</td>
</tr>
<tr>
<td>notifications</td>
<td>Normal but significant conditions (severity=5)</td>
</tr>
<tr>
<td>warnings</td>
<td>Normal but significant conditions (severity=4)</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58>logging monitor warnings

rfs4000-229D58>show logging

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

Log Buffer (522 bytes):

Apr 30 12:24:12 2014: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'superuser' from 'pts/1'
Apr 30 12:24:12 2014: %AUTH-4-WARNING: login[2901]: login failed for 'superuser' on 'pts/1'
Apr 30 12:24:01 2014: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'exit' from 'pts/1'
Apr 30 12:24:01 2014: %AUTH-4-WARNING: login[2901]: login failed for 'exit' on 'pts/1'
rfs4000-229D58>
<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Resets terminal lines logging levels</td>
</tr>
</tbody>
</table>
### 2.1.15 mint

**User Exec Commands**

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

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```plaintext
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**

- **mint ping <MINT-ID> {{count <1-10000>|size <1-64000>|timeout <1-10>}}**
  
<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></td>
<td>• &lt;MINT-ID&gt; — Specify the destination device’s MiNT ID.</td>
</tr>
<tr>
<td>count &lt;1-10000&gt;</td>
<td>Optional. Sets the pings to the MiNT destination</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-10000&gt; — Specify a value from 1 - 10000. The default is 3.</td>
</tr>
<tr>
<td>size &lt;1-64000&gt;</td>
<td>Optional. Sets the MiNT payload size in bytes</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64000&gt; — Specify a value from 1 - 640000 bytes. The default is 64 bytes.</td>
</tr>
<tr>
<td>timeout &lt;1-10&gt;</td>
<td>Optional. Sets a response time in seconds</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-10&gt; — Specify a value from 1 sec - 10 sec. The default is 1 second.</td>
</tr>
</tbody>
</table>

- **mint traceroute <MINT-ID> {{destination-port <1-65535>|max-hops <1-255>|source-port <1-65535>|timeout <1-255>}}**
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute &lt;MINT-ID&gt;</td>
<td>Prints the route packets trace to a device</td>
</tr>
<tr>
<td></td>
<td>• &lt;MINT-ID&gt; — Specify the destination device’s MiNT ID.</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></td>
<td>• &lt;1-65535&gt; — Specify a value from 1 - 65535. The default port is 45.</td>
</tr>
<tr>
<td>max-hops &lt;1-255&gt;</td>
<td>Optional. Sets the maximum number of hops a traceroute packet traverses in the forward direction</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-255&gt; — Specify a value from 1 - 255. The default is 30.</td>
</tr>
<tr>
<td>source-port &lt;1-65535&gt;</td>
<td>Optional. Sets the ECMP source port</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; — Specify a value from 1 - 65535. The default port is 45.</td>
</tr>
<tr>
<td>timeout &lt;1-255&gt;</td>
<td>Optional. Sets the minimum response time period in seconds</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-255&gt; — Specify a value from 1 sec - 255 sec. The default is 30 seconds.</td>
</tr>
</tbody>
</table>
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>
2.1.16 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

no [adoption|captive-portal|crypto|debug|logging|mac-user-db|page|service|terminal|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>}}

no logging monitor

no mac-user-db user [<USER-NAME>|all]

no page

no service [ap300|enable|locator]

no service ap300 locator <MAC>

no service enable [l2tpv3|radiusd]

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 {on <DEVICE-OR-DOMAIN-NAME>}{filter [wlan <WLAN-NAME>]}

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

Parameters

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no adoption {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>Resets the adoption status of a specified device or all devices</td>
</tr>
<tr>
<td>• &lt;DEVICE-OR-DOMAIN-NAME&gt; — Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain. If an RF Domain is specified, the system resets status of all adopted devices within the specified domain.</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>captive-portal &lt;CAPTIVE-PORTAL-NAME&gt;</code></td>
<td>Disconnects clients of the captive portal identified by the <code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> keyword.</td>
</tr>
<tr>
<td><code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> – Specify the captive portal name.</td>
<td></td>
</tr>
<tr>
<td><code>mac &lt;MAC&gt;</code></td>
<td>Disconnects a client specified by its MAC address.</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;</code> – Specify the client's MAC address.</td>
<td></td>
</tr>
<tr>
<td><code>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>Optional. Disconnects clients on a specified device or RF Domain.</td>
</tr>
<tr>
<td><code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code> – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
<td></td>
</tr>
<tr>
<td>`no crypto pki [server</td>
<td>trustpoint] &lt;TRUSTPOINT-NAME&gt; {del-key {on &lt;DEVICE-NAME&gt;}}`</td>
</tr>
<tr>
<td>`[server</td>
<td>trustpoint] &lt;TRUSTPOINT-NAME&gt;`</td>
</tr>
<tr>
<td><code>server</code> – Deletes server certificates.</td>
<td></td>
</tr>
<tr>
<td><code>trustpoint</code> – Deletes a trustpoint and its associated certificates.</td>
<td></td>
</tr>
<tr>
<td>The following keyword is common to the ‘server’ and ‘trustpoint’ parameters:</td>
<td></td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code> – Deletes a trustpoint or its server certificate. Specify the trustpoint name.</td>
<td></td>
</tr>
<tr>
<td><code>del-key {on &lt;DEVICE-NAME&gt;}</code></td>
<td>Optional. Deletes the private key associated with a server certificate or trustpoint. The operation fails if the private key is in use by other trustpoints.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code> – Optional. Deletes the private key on a specified device.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
<tr>
<td><code>no logging monitor</code></td>
<td>Resets terminal lines message logging levels.</td>
</tr>
<tr>
<td>`no mac-user-db user [&lt;USER-NAME&gt;</td>
<td>all]`</td>
</tr>
<tr>
<td><code>&lt;USER-NAME&gt;</code></td>
<td>Deletes the user, identified by the <code>&lt;USER-NAME&gt;</code> keyword, from the MAC registration user database.</td>
</tr>
<tr>
<td><code>&lt;USER-NAME&gt;</code> – Specify the username.</td>
<td></td>
</tr>
<tr>
<td><code>all</code></td>
<td>Deletes all users from the MAC registration user database.</td>
</tr>
<tr>
<td><code>no page</code></td>
<td>Resets paging to its default. Disabling paging displays the CLI command output at once, instead of page by page.</td>
</tr>
</tbody>
</table>
- no service ap300 locator <MAC>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no service</td>
<td>Disables device LEDs in the WLAN. It also resets the CLI table expand and MiNT protocol configurations.</td>
</tr>
<tr>
<td>no ap300 locator</td>
<td>Disables LEDs on a specified AP300</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>• &lt;MAC&gt; – Specify the AP300’s MAC address.</td>
</tr>
<tr>
<td>Note:</td>
<td>If no MAC address is specified, the system disables LEDs on all AP300s.</td>
</tr>
</tbody>
</table>

- no service enable [l2tpv3|radiusd]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no service</td>
<td>Disables specified services or features</td>
</tr>
<tr>
<td>enable [l2tpv3</td>
<td>radiusd]</td>
</tr>
<tr>
<td>l2tpv3 –</td>
<td>Disables L2TPV3</td>
</tr>
<tr>
<td>radiusd –</td>
<td>Disables loading of the RADIUS server on low memory devices</td>
</tr>
</tbody>
</table>

- no service locator {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no service</td>
<td>Disables LEDs on a specified device or all devices in the WLAN. It also resets the CLI table expand and MiNT protocol configurations.</td>
</tr>
<tr>
<td>locator {on &lt;DEVICE-NAME&gt;}</td>
<td>Disables LEDs on a specified device</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>Note:</td>
<td>If no device name is specified, the system disables LEDs on all devices in the WLAN.</td>
</tr>
</tbody>
</table>

- no terminal [length|width]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no terminal [length</td>
<td>width]</td>
</tr>
<tr>
<td>length –</td>
<td>Resets the number of lines displayed on the terminal window to its default</td>
</tr>
<tr>
<td>width –</td>
<td>Resets the width of the terminal window to its default</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no virtual-machine assign-usb-ports</td>
<td>Reverts ports assigned for virtual-machines back to WiNG</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Reverts virtual-machine assigned ports on a specified device</td>
</tr>
<tr>
<td>Note:</td>
<td>This command is available only on the NX45XX, NX65XX, NX9500, and NX9510 series service platforms.</td>
</tr>
<tr>
<td>Optional.</td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no wireless client all</td>
<td>Disassociates all clients on a specified device or domain</td>
</tr>
<tr>
<td>filter [wlan &lt;WLAN-NAME&gt;]</td>
<td>Optional. Specifies additional client selection filter</td>
</tr>
<tr>
<td>• wlan –</td>
<td>Filters clients on a specified WLAN</td>
</tr>
<tr>
<td>• &lt;WLAN-NAME&gt; –</td>
<td>Specify the WLAN name.</td>
</tr>
</tbody>
</table>
### no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}

Disassociates all wireless clients on a specified device or domain
- on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.

<table>
<thead>
<tr>
<th>filter [wlan &lt;WLAN-NAME&gt;]</th>
<th>The following are optional filter parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter – Optional. Specifies additional client selection filter</td>
<td></td>
</tr>
<tr>
<td>wlan – Filters clients on a specified WLAN</td>
<td></td>
</tr>
<tr>
<td>&lt;WLAN-NAME&gt; – Specify the WLAN name.</td>
<td></td>
</tr>
</tbody>
</table>

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

Disassociates a single wireless client on a specified device or RF Domain
- mac <MAC> – Specify the wireless client’s MAC address in the AA-BB-CC-DD-EE-FF format.

| on <DEVICE-OR-DOMAIN-NAME> | Optional. Specifies the name of the AP, wireless controller, service platform, or RF Domain to which the specified client is associated |

#### 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
rfs7000-37FABE>no service cli-tables-expand line
```

#### Related Commands
- **auto-provisioning-policy** Resets the adoption state of a device and all devices adopted to it
- **captive portal** Manages captive portal clients
- **crypto** Enables digital certificate configuration and RSA Keypair management.
- **logging** Modifies message logging settings
- **page** Resets paging to its default
- **service** Performs different functions depending on the parameter passed
- **terminal** Sets the length or the number of lines displayed within the terminal window
- **virtual-machine** Installs, configures, and monitors the status of third-party virtual machines (VMs). This command is specific to the NX45XX, NX65XX, NX9500, NX9600, and NX9510 series service platforms.
- **wireless-client** Manages wireless clients
2.1.17 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax
page

Parameters
None

Examples
rfs7000-37FABE>page
rfs7000-37FABE>

Related Commands

| no         | Disables device paging |
2.1.18 ping

User Exec Commands

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

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}
```

Parameters

- ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Specify the destination IP address or hostname. When entered without any parameters, this command prompts for an IP address or a hostname.</td>
</tr>
<tr>
<td>count &lt;1-10000&gt;</td>
<td>Optional. Sets the pings to the specified destination</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-10000&gt; – Specify a value from 1 - 10000. The default is 5.</td>
</tr>
<tr>
<td>dont-fragment {count</td>
<td>size}</td>
</tr>
<tr>
<td></td>
<td>• count &lt;1-10000&gt; – Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5.</td>
</tr>
<tr>
<td></td>
<td>• size &lt;1-64000&gt; – Optional. Sets the ping payload size from 1 - 64000 bytes. The default is 100 bytes.</td>
</tr>
<tr>
<td>size &lt;1-64000&gt;</td>
<td>Optional. Sets the ping payload size in bytes</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64000&gt; – Specify the ping payload size from 1 - 64000. The default is 100 bytes.</td>
</tr>
</tbody>
</table>

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>
```
2.1.19 ssh

User Exec Commands

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

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

ssh <IP/HOSTNAME> <USER-NAME>

Parameters

- ssh <IP/HOSTNAME> <USER-NAME>

<table>
<thead>
<tr>
<th>&lt;IP/HOSTNAME&gt;</th>
<th>Specify the remote system's IP address or hostname.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify the name of the user requesting SSH connection with the remote system.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE>ssh 172.16.10.4 admin
The authenticity of host '172.16.10.4 (172.16.10.4)' can't be established.
Are you sure you want to continue connecting (yes/no)?
2.1.20 telnet

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

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

Parameters

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

<table>
<thead>
<tr>
<th>&lt;IP/HOSTNAME&gt;</th>
<th>Configures the destination remote system’s IP address or hostname. The Telnet session is established between the connecting system and the remote system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TCP-PORT&gt;</td>
<td>Optional. Specify the Transmission Control Protocol (TCP) port number.</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58>telnet 192.168.13.23

Entering character mode
Escape character is '^]'.

AP7131 release 5.5.6.0-006D
ap7131-11B6C4 login:
2.1.21 terminal

Sets the length or the number of lines displayed within the terminal window

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

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 &lt;0-512&gt;</td>
<td>Sets the number of lines displayed on a terminal window</td>
</tr>
<tr>
<td>width &lt;0-512&gt;</td>
<td>Sets the width (the number of characters displayed) 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 and length of the terminal window
2.1.22 time-it

User Exec Commands

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

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

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#
2.1.23 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

traceroute <LINE>

Parameters

- traceroute <LINE>

<table>
<thead>
<tr>
<th>traceroute &lt;LINE&gt;</th>
<th>Traces the route to a destination IP address or hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;LINE&gt;</td>
<td>- Specify a traceroute argument. For example, “service traceroute-h”.</td>
</tr>
</tbody>
</table>

Examples

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

Usage: traceroute [-FIdlnvr] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q nqueries]
          [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
          [-z pausemsecs] HOST [data size]
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 (8 max)

rfs7000-37FABE>
```

```
rfs7000-37FABE>traceroute 172.16.10.1
traceroute to 172.16.10.1 (172.16.10.1), 30 hops max, 38 byte packets
  1  172.16.10.1 (172.16.10.1)  0.423 ms  0.145 ms  0.225 ms
rfs7000-37FABE>
```
### 2.1.24 watch

#### User Exec Commands

Repeats the specified CLI command at periodic intervals

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

#### Syntax

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

#### Parameters

- **watch**
  - Repeats a CLI command at a specified interval (in seconds)
- **<1-3600>**
  - Select an interval from 1 - 3600 sec. Pressing CTRL-Z halts execution of the command.
- **<LINE>**
  - Specify the CLI command.

#### Examples

```
rfs7000-37FABE>watch 45 page
```

```
rfs7000-37FABE>watch 45 ping 172.16.10.2
PING 172.16.10.2 (172.16.10.2): 100 data bytes
108 bytes from 172.16.10.2: seq=0 ttl=64 time=0.725 ms
108 bytes from 172.16.10.2: seq=1 ttl=64 time=0.464 ms
108 bytes from 172.16.10.2: seq=2 ttl=64 time=0.458 ms
108 bytes from 172.16.10.2: seq=3 ttl=64 time=0.378 ms
108 bytes from 172.16.10.2: seq=4 ttl=64 time=0.364 ms
--- 172.16.10.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.364/0.477/0.725 ms
rfs7000-37FABE>
```
2.1.25 **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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

`exit`

**Parameters**

None

**Examples**

`rfs7000-37FABE>exit`
2.1.26 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, NX6500, NX6524

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#
2.1.27 virtual-machine

User Exec Commands

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

In addition to the shipped VMs, the NX45XX, NX65XX, NX9500, NX9600 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 are:

- 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, NX6500, NX6524, NX9500, NX9600, NX9510

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}|team-urc|team-rls|team-vowlan]

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]}{vif-to-vmif <VIF-INDEX> [VMIF-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}{on <DEVICE-NAME>}
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-machine stop hard</td>
<td>Stops the VM and optionally reassigns the USB ports to WiNG. The VM image is stored in an archive on the specified device.</td>
</tr>
<tr>
<td>virtual-machine uninstall</td>
<td>Uninstalls the VM from the specified device.</td>
</tr>
<tr>
<td>assign-usb-ports team-vowlan</td>
<td>Assigns USB ports to TEAM-VoWLAN on a specified device. The port assignment can be reverted using the <code>no</code> option. The TEAM-RLS VM cannot be installed if USB ports are assigned to TEAM-VoWLAN.</td>
</tr>
<tr>
<td>virtual-machine console</td>
<td>Connects to the VM's console. The console options include: &lt;VM-NAME&gt; – Connects to the console of the VM identified by the &lt;VM-NAME&gt; keyword. Team-Urc – Connects to the VM TEAM Unified Retail Communication's (URC) (IP-PBX) console.</td>
</tr>
<tr>
<td>virtual-machine export</td>
<td>Exports an existing VM image and settings. Use this command to export the VM to another NX45XX or NX65XX device in the same domain. The export path can be specified as a URL or file name.</td>
</tr>
</tbody>
</table>
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**
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)
  - 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**
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.

Contd...
virtual-machine install

```
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

```
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.

**Note:** 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> vif-to-vmif <VIF-INDEX> <VMIF-INDEX> vnc [disable|enable] [<VM-NAME|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>virtual-machine set</th>
<th>Configures the VM settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>autostart – Specifies whether to autostart the VM on system reboot</td>
<td></td>
</tr>
<tr>
<td>ignore – Enables autostart on each system reboot</td>
<td></td>
</tr>
<tr>
<td>start – Disables autostart</td>
<td></td>
</tr>
<tr>
<td>memory – Defines the VM memory size</td>
<td></td>
</tr>
<tr>
<td>&lt;512-8192&gt; – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.</td>
<td></td>
</tr>
<tr>
<td>vcpus – Specifies the number of VCPUS for this VM</td>
<td></td>
</tr>
<tr>
<td>&lt;1-4&gt; – Specify the number of VCPUS from 1- 4.</td>
<td></td>
</tr>
<tr>
<td>vif-count – Configures or resets the VM’s VIFs</td>
<td></td>
</tr>
<tr>
<td>&lt;0-2&gt; – Specify the VIF number from 0 - 2.</td>
<td></td>
</tr>
<tr>
<td>vif-mac – Configures the MAC address of the selected virtual network interface</td>
<td></td>
</tr>
<tr>
<td>&lt;1-2&gt; – Select the VIF</td>
<td></td>
</tr>
<tr>
<td>&lt;1-8&gt; – Specify the MAC index for the selected VIF</td>
<td></td>
</tr>
<tr>
<td>&lt;MAC&gt; – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.</td>
<td></td>
</tr>
</tbody>
</table>

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.

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 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, 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

Contd...
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

**virtual-machine start**

Starts the VM, based on the parameters passed. Select one of the following options:

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

**virtual-machine stop**

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.

**Note:** The option 'hard' forces the selected VM to shutdown.

**virtual-machine uninstall**

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 wing-memory <12288-32739>`
- `virtual-machine set memory <512-8192> adsp {on <DEVICE-NAME>}`
- `virtual-machine [start|stop] adsp {on <DEVICE-NAME>}`
- `virtual-machine uninstall adsp {on <DEVICE-NAME>}`

**NOTE:** On an NX9XXX, 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 NX9XXX series service platform.

---

**Parameters NX9500 and NX9510**

- `virtual-machine console adsp`

<table>
<thead>
<tr>
<th><code>virtual-machine console</code></th>
<th>Connects to the <em>Air-Defense Services Platform</em> (ADSP) VM’s management console</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When ADSP is running on the NX9500 and NX9510 model service platforms, WiNG communicates with ADSP using a <em>single sign-on</em> (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 <em>tree-node</em>.</td>
</tr>
</tbody>
</table>
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.

**Note:** 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
Aug 20 15:12:41 2014: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1 127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 192 "-" ",",
-03-5.5.6.0-006D.img
Aug 20 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)........Aug 20 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 <DEVICE-NAME>}

Sets the ADSP VM’s disk size (in GB). Specify a value from 100 - 500 GB.

- 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:** Stop the ADSP VM before executing this command.

virtual-machine set memory <512-8192> adsp {on <DEVICE-NAME>}

Modifies the ADSP VM’s memory. Specify a value from 512 - 8192 MB.

- 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

  **Note:** 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.

  **Note:** 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

  - 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).

nx4500-5CF602B>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
NOTE: Use the show > virtual-machine > [configuration|debugging|export|statistics] command to view installed VM details.
CHAPTER 3
PRIVILEGED EXEC MODE COMMANDS

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 from one file to another
create-cluster              Create a cluster
crypto                      Encryption related commands
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
disable                     Turn on privileged mode command
erase                       Erase a filesystem
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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>more</td>
<td>Display the contents of a file</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>page</td>
<td>Toggle paging</td>
</tr>
<tr>
<td>ping</td>
<td>Send ICMP echo messages</td>
</tr>
<tr>
<td>pwd</td>
<td>Display current directory</td>
</tr>
<tr>
<td>raid</td>
<td>RAID operations</td>
</tr>
<tr>
<td>re-elect</td>
<td>Perform re-election</td>
</tr>
<tr>
<td>reload</td>
<td>Halt and perform a warm reboot</td>
</tr>
<tr>
<td>remote-debug</td>
<td>Troubleshoot remote system(s)</td>
</tr>
<tr>
<td>rename</td>
<td>Rename a file</td>
</tr>
<tr>
<td>revert</td>
<td>Revert changes</td>
</tr>
<tr>
<td>rmdir</td>
<td>Delete a directory</td>
</tr>
<tr>
<td>self</td>
<td>Config context of the device currently logged into</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>smart-cache</td>
<td>Content Cache Operation</td>
</tr>
<tr>
<td>ssh</td>
<td>Open an ssh connection</td>
</tr>
<tr>
<td>telnet</td>
<td>Open a telnet connection</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
</tr>
<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>upgrade</td>
<td>Upgrade software image</td>
</tr>
<tr>
<td>upgrade-abort</td>
<td>Abort an ongoing upgrade</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>#
3.1 Privileged Exec Mode Commands

Table 3.1 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 3-5</td>
</tr>
<tr>
<td>boot</td>
<td>Specifies the image used after reboot</td>
<td>page 3-7</td>
</tr>
<tr>
<td>captive-portal-page-upload</td>
<td>Uploads captive portal advanced pages</td>
<td>page 3-8</td>
</tr>
<tr>
<td>cd</td>
<td>Changes the current directory</td>
<td>page 3-10</td>
</tr>
<tr>
<td>change-passwd</td>
<td>Changes the password of a logged user</td>
<td>page 3-11</td>
</tr>
<tr>
<td>clear</td>
<td>Clears parameters, cache entries, table entries, and other similar entries</td>
<td>page 3-12</td>
</tr>
<tr>
<td>clock</td>
<td>Configures the system clock</td>
<td>page 3-22</td>
</tr>
<tr>
<td>cluster</td>
<td>Initiates a cluster context</td>
<td>page 3-23</td>
</tr>
<tr>
<td>configure</td>
<td>Enters the configuration mode</td>
<td>page 3-24</td>
</tr>
<tr>
<td>connect</td>
<td>Begins a console connection to a remote device</td>
<td>page 3-25</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 3-26</td>
</tr>
<tr>
<td>create-cluster</td>
<td>Creates a new cluster on a specified device</td>
<td>page 3-27</td>
</tr>
<tr>
<td>crypto</td>
<td>Enables encryption</td>
<td>page 3-29</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a specified file from the system</td>
<td>page 3-40</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade parameters</td>
<td>page 3-41</td>
</tr>
<tr>
<td>diff</td>
<td>Displays the differences between two files</td>
<td>page 3-51</td>
</tr>
<tr>
<td>dir</td>
<td>Displays the list of files on a file system</td>
<td>page 3-52</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the privileged mode command set</td>
<td>page 3-53</td>
</tr>
<tr>
<td>edit</td>
<td>Edits a text file</td>
<td>page 3-54</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on (enables) the privileged mode commands set</td>
<td>page 3-55</td>
</tr>
<tr>
<td>erase</td>
<td>Erases a file system</td>
<td>page 3-56</td>
</tr>
<tr>
<td>halt</td>
<td>Halts a device (access point, wireless controller, or service platform)</td>
<td>page 3-57</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 3-58</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Establishes or brings down Layer 2 Tunneling Protocol Version 3 (L2TPV3) tunnels</td>
<td>page 3-59</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging parameters</td>
<td>page 3-61</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocols</td>
<td>page 3-62</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>mkdir</code></td>
<td>Creates a new directory in the file system</td>
<td>page 3-64</td>
</tr>
<tr>
<td><code>more</code></td>
<td>Displays the contents of a file</td>
<td>page 3-65</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Reverts a command or sets values to their default</td>
<td>page 3-66</td>
</tr>
<tr>
<td><code>page</code></td>
<td>Toggles a device’s (access point, wireless controller, or service platform) paging function</td>
<td>page 3-71</td>
</tr>
<tr>
<td><code>ping</code></td>
<td>Sends ICMP echo messages to a user-specified location</td>
<td>page 3-72</td>
</tr>
<tr>
<td><code>pwd</code></td>
<td>Displays the current directory</td>
<td>page 3-73</td>
</tr>
<tr>
<td><code>re-elect</code></td>
<td>Re-elects the tunnel controller (wireless controller, service platform, or access point)</td>
<td>page 3-74</td>
</tr>
<tr>
<td><code>reload</code></td>
<td>Halts a device (wireless controller, service platform, or access point) and performs a warm reboot</td>
<td>page 3-75</td>
</tr>
<tr>
<td><code>rename</code></td>
<td>Renames a file in the existing file system</td>
<td>page 3-76</td>
</tr>
<tr>
<td><code>rmdir</code></td>
<td>Deletes an existing file from the file system</td>
<td>page 3-77</td>
</tr>
<tr>
<td><code>self</code></td>
<td>Displays the configuration context of the device</td>
<td>page 3-78</td>
</tr>
<tr>
<td><code>ssh</code></td>
<td>Connects to another device using a secure shell</td>
<td>page 3-79</td>
</tr>
<tr>
<td><code>telnet</code></td>
<td>Opens a Telnet session</td>
<td>page 3-80</td>
</tr>
<tr>
<td><code>terminal</code></td>
<td>Sets the length and width of the terminal window</td>
<td>page 3-81</td>
</tr>
<tr>
<td><code>time-it</code></td>
<td>Verifies the time taken by a particular command between request and response</td>
<td>page 3-82</td>
</tr>
<tr>
<td><code>traceroute</code></td>
<td>Traces the route to a defined destination</td>
<td>page 3-83</td>
</tr>
<tr>
<td><code>upgrade</code></td>
<td>Upgrades the software image</td>
<td>page 3-84</td>
</tr>
<tr>
<td><code>upgrade-abort</code></td>
<td>Aborts an ongoing software image upgrade</td>
<td>page 3-85</td>
</tr>
<tr>
<td><code>watch</code></td>
<td>Repeats a specified CLI command at a periodic interval</td>
<td>page 3-86</td>
</tr>
<tr>
<td><code>smart-cache</code></td>
<td>Pre-fetches content cache from the specified list of URLs. This command is specific to the NX45XX and NX65XX series service platforms.</td>
<td>page 3-88</td>
</tr>
<tr>
<td><code>virtual-machine</code></td>
<td>Installs, configures, and monitors the status of virtual machines (VMs). This command is specific to the NX45XX, NX65XX, NX9500, and NX9510 series service platforms.</td>
<td>page 3-89</td>
</tr>
<tr>
<td><code>raid</code></td>
<td>Enables RAID management. This command is specific to the NX9500 series service platforms.</td>
<td>page 3-99</td>
</tr>
</tbody>
</table>
### 3.1.1 archive

*Privileged Exec Mode Commands*

Manages file archive operations

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9600, NX9510

#### 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>]**
  - `tar` manipulates (creates, lists, or extracts) a tar file
  - `/table` lists the files in a tar file
  - `<FILE>` defines a tar filename
  - `<URL>` sets the tar file URL

- **archive tar /create [<FILE>|<URL>] <FILE>**
  - `tar` manipulates (creates, lists, or extracts) a tar file
  - `/create` creates a tar file
  - `<FILE>` defines tar filename
  - `<URL>` sets the tar file URL

- **archive tar /xtract [<FILE>|<URL>] <DIR>**
  - `tar` manipulates (creates, lists, or extracts) a tar file
  - `/xtract` extracts content from a tar file
  - `<FILE>` defines tar filename
  - `<URL>` sets the tar file URL
  - `<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/?

```
  rfs4000-229D58# dir flash:/
  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

  rfs4000-229D58#

  rfs4000-229D58# archive tar /create flash:/out.tar flash:/log
  log/ 
  log/cfgd.log 
  log/cfgd.log.1 
  log/vlan-usage.log 
  log/anald.log 
  log/anald.startup 
  log/dpd2.log 
  log/dpd2.startup 
  log/upgrade.log 
  log/messages.log 
  log/startup.log 
  log/hotplug/ 
  log/hotplug/events 
  log/radius/ 

  rfs4000-229D58#

  rfs4000-229D58# dir flash:/
  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#
```
3.1.2 boot

Specifies the image used after reboot

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

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

Parameters

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

<table>
<thead>
<tr>
<th>System</th>
<th>Specifies the image used after a device reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>primary — Uses the primary image after reboot</td>
</tr>
<tr>
<td>secondary</td>
<td>secondary — Uses the secondary image after reboot</td>
</tr>
</tbody>
</table>

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

Examples

rfs4000-229D58#show boot

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>BUILD DATE</th>
<th>INSTALL DATE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary</td>
<td>06:29:2014 00:36:59</td>
<td>06:30:2014 08:56:11</td>
<td>5.5.6.0-004D</td>
</tr>
</tbody>
</table>

Current Boot: Primary
Next Boot: Primary
Software Fallback: Enabled

rfs4000-229D58#boot system secondary

Updated system boot partition

rfs4000-229D58#

rfs4000-229D58#show boot

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>BUILD DATE</th>
<th>INSTALL DATE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary</td>
<td>06:29:2014 00:36:59</td>
<td>06:30:2014 08:56:11</td>
<td>5.5.6.0-004D</td>
</tr>
</tbody>
</table>

Current Boot: Primary
Next Boot: Secondary
Software Fallback: Enabled

rfs4000-229D58#
### 3.1.3 captive-portal-page-upload

#### Privileged Exec Mode Commands

Uploads captive portal advanced pages

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

#### Syntax

- `captive-portal-page-upload [<CAPTIVE-PORTAL-NAME>|cancel-upload|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 load-file <CAPTIVE-PORTAL-NAME> <URL>`

#### Parameters

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

- `captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME]|all] {from-controller} {(upload-time <TIME>)}`
  - Uploads advanced pages specified by the `<CAPTIVE-PORTAL-NAME>` parameter
    - `<CAPTIVE-PORTAL-NAME>` — Specify captive portal name (should be existing and configured).
  - `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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal-page-upload</td>
<td>Uploads captive portal pages to specified APs.</td>
</tr>
<tr>
<td>cancel-upload</td>
<td>Cancels scheduled AP uploads.</td>
</tr>
<tr>
<td>load-file</td>
<td>Loads captive portal advanced pages.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58# captive-portal-page-upload test1 00-04-96-4A-A7-08 upload-time 03/01/2014-12:30
---------------------------------+---------------------------------+---------------------------------|
CONTROLLER                      | STATUS                         | MESSAGE                        |
--------------------------------|--------------------------------|---------------------------------|
00-23-68-22-9D-58               | Fail                           | Failed to initiate page upload  |
--------------------------------|--------------------------------|---------------------------------|
rfs4000-229D58#                 |
```

```
rfs4000-229D58# captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08
---------------------------------+---------------------------------+---------------------------------|
CONTROLLER                      | STATUS                         | MESSAGE                        |
--------------------------------|--------------------------------|---------------------------------|
00-23-68-22-9D-58               | Success                        | Cancelled upgrade of 1 APs      |
--------------------------------|--------------------------------|---------------------------------|
rfs4000-229D58#                 ```
3.1.4  cd

Privileged Exec Mode Commands

Changes the current directory

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

cd {<DIR>}

Parameters

- cd {<DIR>}

| <DIR> | Optional. Changes the current directory to <DIR>. If a directory name is not provided, the system displays the current directory. |

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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

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#
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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

NOTE: Refer to the interface details below when using clear

- ge <index> – RFS4000 supports 5 GEs, RFS6000 supports 8 GEs, RFS7000 supports 4 GEs, and NX45XX and NX65XX series support 24 GEs
- me1 – Available in both RFS7000 and RFS6000
- up1– Uplink interface on RFS4000

Syntax

clear [arp-cache|cdp|counters|crypto|event-history|firewall|gre|ip|l2tpv3-stats|license|lldp|logging|mac-address-table|mint|role|rtls|smart-cache|spanning-tree|vrrp]
clear arp-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 <1-5>|me1|port-channel <1-3>|pppoe1|vlan <1-4094>|wwan1]
clear counters radio {<MAC/HOSTNAME>|on}
clear counters radio {<MAC/HOSTNAME> <1-3>} {(on <DEVICE-OR-DOMAIN-NAME>)}
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] {on <DEVICE-NAME>}
clear gre stats {on <DEVICE-NAME>}
clear ip [dhcp|ospf]
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}
clear l2tpv3-stats tunnel <L2TPV3-TUNNEL-NAME> {on <DEVICE-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>}

NOTE: Refer to the interface details below when using clear

- ge <index> – RFS4000 supports 5 GEs, RFS6000 supports 8 GEs, RFS7000 supports 4 GEs, and NX45XX and NX65XX series support 24 GEs
- me1 – Available in both RFS7000 and RFS6000
- up1– Uplink interface on RFS4000
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>|vmf <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] \{on <DEVICE-OR-DOMAIN-NAME>\}
clear rtls [aeroscout|ekahau] \{<DEVICE-NAME> \{on <DEVICE-OR-DOMAIN-NAME>\}\}
clear spanning-tree detected-protocols \{interface|on <DEVICE-NAME>\}
clear spanning-tree detected-protocols \{interface \<INTERFACE-NAME>|ge <1-5>|me1|port-channel <1-3>|pppoel|vlan <1-4094>|wwan1\} \{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**

- **clear arp-cache \{on <DEVICE-NAME>\}**

<table>
<thead>
<tr>
<th>arp-cache</th>
<th>Clears Address Resolution Protocol (ARP) cache entries on a device</th>
</tr>
</thead>
</table>
| 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 [cdp|lldp] neighbors \{on <DEVICE-NAME>\}**

| cdp | Clears Cisco Discovery Protocol (CDP) table entries |
| ldp | Clears Link Layer Discovery Protocol (LLDP) neighbor 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 [all|bridge|router|thread]**

<table>
<thead>
<tr>
<th>counters</th>
<th>Clears counters on a system</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears all counters irrespective of the interface type</td>
</tr>
<tr>
<td>bridge</td>
<td>Clears bridge counters</td>
</tr>
<tr>
<td>router</td>
<td>Clears router counters</td>
</tr>
<tr>
<td>thread</td>
<td>Clears per-thread counters</td>
</tr>
</tbody>
</table>

- **clear counters \{ap|wireless-client\} \{<MAC>\} \{on <DEVICE-OR-DOMAIN-NAME>\}**

<p>| counters {ap|wireless-client} | Clears counters on a system |
| --- | --- |
| ap | Clears access point wireless counters |
| wireless-client | Clears wireless client counters |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters interface</td>
<td>Clears interface counters for a specified interface.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;INTERFACE-NAME&gt;</td>
<td>Clears a specified interface counters. Specify the interface name.</td>
</tr>
<tr>
<td>all</td>
<td>Clears all interface counters</td>
</tr>
<tr>
<td>ge &lt;1-5&gt;</td>
<td>Clears GigabitEthernet interface counters. Specify the GigabitEthernet interface index from 1 - 5.</td>
</tr>
<tr>
<td>me1</td>
<td>Clears FastEthernet interface counters</td>
</tr>
<tr>
<td>port-channel &lt;1-3&gt;</td>
<td>Clears port-channel interface counters. Specify the port channel interface index from 1 - 3.</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Clears Point-to-Point Protocol over Ethernet (PPPoE) interface counters</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Clears interface counters. Specify the Switch Virtual Interface (SVI) VLAN ID from 1 - 4094.</td>
</tr>
<tr>
<td>wwan1</td>
<td>Clears wireless WAN interface counters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear counters radio</th>
<th>Clears wireless radio counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC/HOSTNAME&gt; &lt;1-3&gt;</td>
<td>Clears counters of a radio identified by the &lt;MAC/HOSTNAME&gt; keyword.</td>
</tr>
<tr>
<td></td>
<td>&lt;MAC/HOSTNAME&gt; – 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</td>
</tr>
<tr>
<td></td>
<td>&lt;1-3&gt; – Optional. Specify the radio index (if not specified as part of the radio ID).</td>
</tr>
<tr>
<td>Note:</td>
<td>The system clears all radio counters, if no MAC address or radio index is specified.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear crypto ike sa</th>
<th>Clears encryption module database</th>
</tr>
</thead>
<tbody>
<tr>
<td>[&lt;IP&gt;</td>
<td>all]</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clear crypto ipsec sa</td>
<td>Clears Internet Key Exchange (IKE) security associations (SAs)</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears IKE SA entries, for a specified peer or all peers, 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>
<tr>
<td>clear event-history</td>
<td>Clears event history cache entries</td>
</tr>
<tr>
<td>clear firewall [dhcp snoop-table</td>
<td>dos stats</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to the DHCP, DOS, and flows parameters:</td>
</tr>
<tr>
<td></td>
<td>on &lt;DEVICE-NAME&gt; – Optional. Clears DHCP snoop table entries, denial of service statistics, or the established firewall sessions 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>
<tr>
<td>clear gre stats</td>
<td>Clears GRE tunnel statistics</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. GRE tunnel 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>
<tr>
<td>clear ip dhcp bindings</td>
<td>Clears a Dynamic Host Configuration Protocol (DHCP) server’s IP address bindings 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>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| `clear ip ospf process {on <DEVICE-NAME>}` | Clears already enabled open shortest path first (OSPF) process and restarts the process on <DEVICE-NAME>. 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.  
  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| `clear l2tpv3-stats tunnel <L2TPV3-TUNNEL-NAME> {on <DEVICE-NAME>|session <SESSION-NAME> {on <DEVICE-NAME>}}` | Clears L2TPv3 tunnel session statistics, clearing all sessions associated with a specified L2TPv3 tunnel or device. Use the following optional parameters to specify a session or device.  
  
  • <L2TPV3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name.  
  
  • on <DEVICE-NAME> – Optional. Clears all sessions associated with the specified L2TPv3 tunnel running on a specified device  
  
  • DEVICE-NAME – Specify the name of the AP, wireless controller, or service platform.  
  
  • session <SESSION-NAME> – Optional. Clears a specified L2TPv3 tunnel session. Specify the session name.  
  
  • 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>}` | Releases or revokes all licenses borrowed by a site controller. Use optional parameters to specify the controller’s name.  
  
  • 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. |
| `clear license lent to <DEVICE-NAME> {on <DEVICE-NAME>}` | NOC controller releases or revokes all licenses loaned to a site controller. Use optional parameters to specify the controller’s name.  
  
  • to <DEVICE-NAME> – Specifies the borrowing controller’s name  
  
  • <DEVICE-NAME> – Specify the controller’s name.  
  
  • 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. |
**clear mac-address-table** {address <MAC>|vlan <1-4094>} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address-table</td>
<td>Clears the MAC address forwarding table</td>
</tr>
<tr>
<td>address &lt;MAC&gt;</td>
<td>Optional. Clears a specified MAC address from the MAC address table.</td>
</tr>
<tr>
<td></td>
<td>• &lt;MAC&gt; – 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</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Optional. Clears all MAC addresses for a specified VLAN</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears a single entry or all MAC entries for the specified VLAN in the MAC address forwarding table 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>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

**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>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address-table</td>
<td>Clears the MAC address forwarding table</td>
</tr>
<tr>
<td>interface</td>
<td>Clears all MAC addresses for the selected interface. Use the options available to specify the interface.</td>
</tr>
<tr>
<td>&lt;IF-NAME&gt;</td>
<td>Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port)</td>
</tr>
<tr>
<td></td>
<td>• &lt;IF-NAME&gt; – Specify the layer 2 interface name.</td>
</tr>
<tr>
<td>ge &lt;1-X&gt;</td>
<td>Clears MAC address forwarding table for the specified GigabitEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-X&gt; – 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>port-channel &lt;1-X&gt;</td>
<td>Clears MAC address forwarding table for the specified port-channel interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-X&gt; – 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>t1e1 &lt;1-4&gt; &lt;1-1&gt;</td>
<td>Clears MAC address forwarding table for the specified T1E1L interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4&gt; – 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><strong>Note:</strong> The T1E1 interfaces are supported only on the NX45XX and NX65XX series service platforms.</td>
</tr>
<tr>
<td>up &lt;1-X&gt;</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>
</tbody>
</table>
### clear mint mlcp history {on <DEVICE-NAME>}

- **mint**: Clears MiNT related information
- **mlcp history**: Clears MiNT Link Creation Protocol (MLCP) client history
- **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>}

- **role ldap-stats**: Clears role based LDAP server statistics
- **on <DEVICE-NAME>**: Optional. Clears role based LDAP server statistics on a specified device
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

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

- **rtls**: Clears Real Time Location Service (RTLS) statistics
- **aeroscout**: Clears RTLS Aeroscout statistics
- **ekahau**: Clears RTLS Ekahau statistics
- **<DEVICE-NAME>**: This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.
  - `<DEVICE-NAME>` – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, or service platform.
- **<DEVICE-OR-DOMAIN-NAME>**: This keyword is common to the ‘aeroscout’ and ‘ekahau’ parameters.
  - `<DEVICE-OR-DOMAIN-NAME>` – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified device or RF Domain. 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 protocols on an interface, and also restarts protocol migration
- **detected-protocols**: Restarts protocol migration
### PRIVILEGED EXEC MODE COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear spanning-tree detected-protocols {interface [&lt;INTERFACE-NAME&gt;</td>
<td>ge &lt;1-5&gt;</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Clears spanning tree protocols on an interface and restarts protocol migration.</td>
</tr>
<tr>
<td>detected-protocols</td>
<td>Restarts protocol migration</td>
</tr>
<tr>
<td>interface [&lt;INTERFACE-NAME&gt;</td>
<td>ge &lt;1-5&gt;</td>
</tr>
<tr>
<td>ge &lt;1-5&gt;</td>
<td>Clears detected spanning tree entries for the selected GigabitEthernet interface.</td>
</tr>
<tr>
<td>me1</td>
<td>Clears FastEthernet interface status</td>
</tr>
<tr>
<td>port-channel &lt;1-3&gt;</td>
<td>Clears detected spanning tree entries for the selected port channel interface.</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Clears detected spanning tree entries for PPPoE interface.</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Clears detected spanning tree entries for the selected VLAN interface.</td>
</tr>
<tr>
<td>wwan1</td>
<td>Clears detected spanning tree entries for wireless WAN interface.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears spanning tree protocol entries on a selected device</td>
</tr>
<tr>
<td>vrrp</td>
<td>Clears Virtual Router Redundancy Protocol (VRRP) statistics for a device</td>
</tr>
<tr>
<td>error-stats {on &lt;DEVICE-NAME&gt;}</td>
<td>Clears global VRRP statistics</td>
</tr>
<tr>
<td>stats {on &lt;DEVICE-NAME&gt;}</td>
<td>Clears VRRP related statistics</td>
</tr>
<tr>
<td>smart-cache storage [all</td>
<td>url-regex &lt;WORD&gt;] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>storage</td>
<td>Clears stored content based on the parameters passed</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>[all</td>
<td>regex &lt;WORD&gt;]</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>on &lt;DEVICE-NAME&gt;</th>
<th>Optional. Clears stored content on a specified device</th>
</tr>
</thead>
<tbody>
<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 crypto ike sa all
rfs4000-229D58#
rfs4000-229D58#show crypto ike sa
```

```
IDX PEER VERSION ENCR ALGO HASH ALGO DH GROUP IKE STATE
Total IKE SAs: 0
```

```
rfs4000-229D58#clear spanning-tree detected-protocols interface port-channel 1
rfs7000-37FABE#clear spanning-tree detected-protocols interface ge 1
rfs4000-229D58#clear lldp neighbors
```

```
rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2014-02-15 14:40:22 UTC' by 'admin'
```

```
2014-01-31 01:07:59     rfs4000-229D58  SYSTEM     CLOCK_RESET          System clock
2014-01-31 01:06:24     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user 'admin' from: '192.168.100.224' authentication successful
2014-01-31 00:58:28     rfs4000-229D58  SYSTEM     CONFIG_COMMIT        Configuration commit by user 'admin' from '192.168.100.225'
2014-01-31 00:49:54     rfs4000-229D58  SYSTEM     LOGIN                Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-01-31 00:49:31     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user 'admin' with privilege 'superuser' from '192.168.100.225'(web)
2014-01-31 00:16:32     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user 'admin' with privilege 'superuser' from '192.168.100.224(web)'
2014-01-31 00:15:36     rfs4000-229D58  SYSTEM     LOGIN                Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-01-30 23:43:10     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user 'admin' from: '192.168.100.224' authentication successful
2014-01-30 03:47:47     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user 'admin' with privilege 'superuser' from '192.168.100.231(web)'
2014-01-30 02:45:08     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user 'admin' from: '192.168.100.231' authentication successful
```

```
rfs4000-229D58#clear event-history
rfs4000-229D58#show event-history
EVENT HISTORY REPORT
```

```
--More--
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#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>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: **9**

nx4500-5CFA2B#
### 3.1.7 clock

- **Privileged Exec Mode Commands**

Sets a device's system clock

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**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>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">HH:MM:SS</a></td>
<td>Sets the current time (in military format hours, minutes and seconds)</td>
</tr>
<tr>
<td>&lt;1-31&gt;</td>
<td>Sets the numerical day of the month</td>
</tr>
<tr>
<td>&lt;MONTH&gt;</td>
<td>Sets the month of the year from Jan - Dec</td>
</tr>
<tr>
<td>&lt;1993-2035&gt;</td>
<td>Sets a valid four digit year from 1993 - 2035</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Sets the clock 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**

```
rfs4000-229D58#clock set 14:45:30 15 Feb 2014
rfs4000-229D58#
rfs4000-229D58#show clock
2014-02-15 14:45:43 UTC
rfs4000-229D58#
```
### 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
cluster start-election
```

**Parameters**

- `cluster start-election`

<table>
<thead>
<tr>
<th>start-election</th>
<th>Starts a new cluster master election</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE#cluster start-election
rfs7000-37FABE#
```

**Related Commands**

- `create-cluster` Creates a new cluster on a specified device
- `join-cluster` Adds a controller, as cluster member, to an existing cluster of devices
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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax
configure {self|terminal}

Parameters
- configure {self|terminal}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>self</td>
<td>Optional. Enables the current device’s configuration mode</td>
</tr>
<tr>
<td>terminal</td>
<td>Optional. Enables configuration from the terminal</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)# configure self
Enter configuration commands, one per line. End with CNTL/Z.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE(config)# 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** — AP300, 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, NX9000, NX9500, NX9510

**Syntax**

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

**Parameters**

- `mint-id <MINT-ID>` — Connects to a remote system using the MiNT ID
  - `<MINT-ID>` – Specify the remote device’s MiNT ID.
- `<REMOTE-DEVICE-NAME>` — Connects to a remote system using its name
  - `<REMOTE-DEVICE-NAME>` – Specify the remote device’s name.

**Examples**

```
rfs4000-229D58# show mint lsp-db
1 LSPs in LSP-db of 68.22.9D.58:
LSP 68.22.9D.58 at level 1, hostname "rfs4000-229D58", 0 adjacencies, seqnum 1073
rfs4000-229D58#

rfs4000-229D58# connect mint-id 68.22.9D.58
Entering character mode
Escape character is '^]'.
RFS4000 release 5.5.6.0-006D
rfs4000-229D58 login: admin
Password:
rfs4000-229D58>

rfs4000-229D58# connect mint-id 19.58.72.58
Entering character mode
Escape character is '"'.
AP5142 release 5.5.6.0-006D
ap5142-587258 login: admin
Password:
### WARNING: Not all configuration changes made through CLI are reflected through GUI. Use CLI to revert back changes that were made through CLI. ###
ap5142-587258>
```
### 3.1.11 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** — AP300, 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, Nexus7500, NX9000, NX9500, NX9600, NX9510

**Syntax**

```plaintext
copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]
```

**Parameters**

- `copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]`

  - `<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.

```plaintext
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.

```plaintext
rfs7000-37FABE#copy tftp://157.235.208.105:/running-config running-config
```
### 3.1.12 create-cluster

**Privileged 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 balance 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
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**

```
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#
```

```
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
```

```
rfs4000-229D58# show context
```

```
! Configuration of RFS4000 version 5.5.6.0-006D
! 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#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cluster</strong></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><strong>join-cluster</strong></td>
<td>Adds a wireless controller, access point, or service platform, as cluster member, to an existing cluster of devices</td>
</tr>
</tbody>
</table>
3.1.13 crypto

Privileged Exec Mode Commands

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by Certificate Authorities (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 CAs identity and configuration parameters.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5000, NX5250, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

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 {on <DEVICE-NAME>}}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase <KEY-PASSPHRASE> {background {on <DEVICE-NAME>}}}
crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {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 {on <DEVICE-NAME>}}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {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] [generate-rsa-key|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|subject-name}
crypto pki export request [generate-rsa-key|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|subject-name}
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> {autogen-subject-name|subject-name}
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background {on <DEVICE-NAME>}}
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {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|subject-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

`crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> 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

`crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <KEY-PASSPHRASE>
on <DEVICE-NAME>}
crypto pki zeroize trustpoint <TRUSTPOINT-NAME>{del-key {on <DEVICE-NAME>}}
on <DEVICE-NAME>}

### Parameters

- **crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}
- **<RSA-KEYPAIR-NAME>** – Specify the RSA Keypair name.
- **<EXPORT-TO-URL>** Specify the RSA Keypair destination address in the following format:
  
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<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
- **background {on <DEVICE-NAME>}** Optional. Performs an export operation in the background. Optionally specify the device to export to.
- **on <DEVICE-NAME>** Optional. Performs an export operation on a specific device.
  - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

- **crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase <KEY-PASSPHRASE>
{background {on <DEVICE-NAME>}|on <DEVICE-NAME>}}
- **<RSA-KEYPAIR-NAME>** – Specify the RSA Keypair name.
- **<EXPORT-TO-URL>** Specify the RSA Keypair destination address in the following format:
  
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<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
- **background {on <DEVICE-NAME>}** Optional. Performs an export operation in the background. Optionally specify the device to export to.
- **on <DEVICE-NAME>** Optional. Performs an export operation on a specific device.
  - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

### key

<table>
<thead>
<tr>
<th>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>export rsa &lt;RSA-KEYPAIR-NAME&gt; Exports an existing RSA Keypair to a specified destination</td>
</tr>
<tr>
<td>• &lt;RSA-KEYPAIR-NAME&gt; – Specify the RSA Keypair name.</td>
</tr>
<tr>
<td>&lt;EXPORT-TO-URL&gt; Specify the RSA Keypair destination address in the following format:</td>
</tr>
<tr>
<td>• tftp://&lt;hostname</td>
</tr>
<tr>
<td>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname</td>
</tr>
<tr>
<td>• sftp://&lt;user&gt;@&lt;hostname</td>
</tr>
<tr>
<td>• http://&lt;hostname</td>
</tr>
<tr>
<td>• cf:/path/file</td>
</tr>
<tr>
<td>• usb&lt;n&gt;:/path/file</td>
</tr>
<tr>
<td>background {on &lt;DEVICE-NAME&gt;} Optional. Performs an export operation in the background. Optionally specify the device to export to.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; Optional. Performs an export operation on a specific 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>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>export rsa Exports a RSA Keypair to a specified destination</td>
</tr>
<tr>
<td>• &lt;RSA-KEYPAIR-NAME&gt; – Specify the RSA Keypair name.</td>
</tr>
<tr>
<td>Command</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>crypto key generate rsa (&lt;RSA-KEYPAIR-NAME&gt;) (&lt;1024-2048&gt;) {on (&lt;DEVICE-NAME&gt;)}</td>
</tr>
<tr>
<td>background {on (&lt;DEVICE-NAME&gt;)}</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
</tr>
<tr>
<td>crypto key import rsa (&lt;RSA-KEYPAIR-NAME&gt;) (&lt;IMPORT-FROM-URL&gt;) {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
</tr>
<tr>
<td>background {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
</tr>
</tbody>
</table>

**<EXPORT-TO-URL>**
- Specify the RSA Keypair destination address in the following format:
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<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
- passphrase – Optional. Encrypts RSA Keypair before exporting
- \(<KEY-PASSPHRASE>\) – Specify a passphrase to encrypt the RSA Keypair.

<DEVICE-NAME>
- Optional. Specifies the name of the AP, wireless controller, or service platform.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto key import rsa</code></td>
<td>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</td>
</tr>
<tr>
<td><code>&lt;RSA-KEYPAIR-NAME&gt;</code></td>
<td>Decrypts and imports a RSA Keypair from a specified source</td>
</tr>
<tr>
<td><code>&lt;IMPORT-FROM-URL&gt;</code></td>
<td>Specify the RSA Keypair source address in the following format:</td>
</tr>
<tr>
<td>{passphrase <code>&lt;KEY-PASSPHRASE&gt;</code>}</td>
<td>ftpp://&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>http://&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;@&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>cf:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb&lt;n&gt;:/path/file</td>
</tr>
<tr>
<td></td>
<td>passphrase – Optional. Decrypts the RSA Keypair before importing it</td>
</tr>
<tr>
<td></td>
<td>&lt;KEY-PASSPHRASE&gt; – Specify the passphrase to decrypt the RSA Keypair.</td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code></td>
<td>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>
<tr>
<td><code>crypto key zeroize rsa</code></td>
<td>Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.</td>
</tr>
<tr>
<td><code>&lt;RSA-KEYPAIR-NAME&gt;</code></td>
<td>Deletes a specified RSA Keypair</td>
</tr>
<tr>
<td></td>
<td>&lt;RSA-KEYPAIR-NAME&gt; – Specify the RSA Keypair name.</td>
</tr>
<tr>
<td><code>force</code></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><code>{on &lt;DEVICE-NAME&gt;}</code></td>
<td>Optional. Deletes all certificates associated with the RSA Keypair on a specified device</td>
</tr>
<tr>
<td><code>&lt;DEVICE-NAME&gt;</code></td>
<td>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><code>crypto pki authenticate</code></td>
<td>Enables Private Key Infrastructure (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Authenticates a trustpoint and imports the corresponding CA certificate</td>
</tr>
<tr>
<td><code>&lt;URL&gt;</code></td>
<td>&lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name.</td>
</tr>
</tbody>
</table>
### crypto pki export request

**generate-rsa-key|use-rsa-key** <RSA-KEYPAIR-NAME>

**autogen-subject-name** (url <EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)

- **<URL>** Specify CA's location in the following format:
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<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

**Note:** The CA certificate is imported from the specified location.

- **background {on <DEVICE-NAME>]** Optional. Performs authentication in the background. Optionally specify a device on which to perform authentication.

- **on <DEVICE-NAME>** Optional. Performs authentication on a specified device
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

- **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>
  - generating 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.

- **url <EXPORT-TO-URL>**
  - background {on <DEVICE-NAME>}
  - on <DEVICE-NAME> Specify the CA's location in the following format:
    - tftp://<hostname|IP>[:port]/path/file
    - ftp://<user>:<passwd>@<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

**Note:** The CSR is exported to the specified location.

- background – Optional. Performs export operation in the background
- on <DEVICE-NAME> – Optional. Performs export operation on a specified device
  - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

- **email <SEND-TO-EMAIL>** Exports CSR to a specified e-mail address
  - <SEND-TO-EMAIL> – Specify the CA's e-mail address.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> subject-name <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>) | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates. Generates a new RSA Keypair or uses an existing RSA Keypair
<p>|                         | - generate-rsa-key – Generates a new RSA Keypair for digital authentication |
|                         | - use-rsa-key – Uses an existing RSA Keypair for digital authentication     |
|                         | - &lt;RSA-KEYPAIR-NAME&gt; – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name. |
| subject-name &lt;COMMON-NAME&gt; | Specifies subject name to identify the certificate                      |
|                         | - &lt;COMMON-NAME&gt; – Sets the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length). |
| &lt;COUNTRY&gt;               | Sets the deployment country code (2 character ISO code)                    |
| &lt;STATE&gt;                 | Sets the state name (2 to 64 characters in length)                         |
| &lt;CITY&gt;                  | Sets the city name (2 to 64 characters in length)                          |
| &lt;ORGANIZATION&gt;          | Sets the organization name (2 to 64 characters in length)                 |
| &lt;ORGANIZATION-UNIT&gt;     | Sets the organization unit (2 to 64 characters in length)                 |
| &lt;EXPORT-TO-URL&gt;         | Specify the CA's location in the following format:                         |
|                         | tftp://&lt;hostname|IP&gt;[port]/path/file                                                           |
|                         | ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname|IP&gt;[port]/path/file                                                            |
|                         | sftp://&lt;user&gt;@&lt;hostname|IP&gt;[port]/path/file                                                              |
|                         | http://&lt;hostname|IP&gt;[port]/path/file                                                              |
|                         | cf:/path/file                                                              |
|                         | usb&lt;n&gt;:/path/file                                                           |
|                         | <strong>Note</strong>: The CSR is exported to the specified location.                   |
|                         | - background – Optional. Performs an export operation in the background     |
|                         | - on &lt;DEVICE-NAME&gt; – Optional. Performs an export operation on a specific device |
|                         | - &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform. |
| email &lt;SEND-TO-EMAIL&gt;   | Exports CSR to a specified e-mail address                                   |
|                         | - &lt;SEND-TO-EMAIL&gt; – Specify the CA's e-mail address.                       |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto pki export trustpoint</code></td>
<td>Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key.</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Specify the trustpoint name.</td>
</tr>
<tr>
<td><code>&lt;EXPORT-TO-URL&gt;</code></td>
<td>Specify the destination address in the following format:</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;@&lt;hostname/IP&gt;[:port]//path/file</td>
</tr>
<tr>
<td></td>
<td>http://&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>cf://path/file</td>
</tr>
<tr>
<td></td>
<td>usb&lt;n&gt;://path/file</td>
</tr>
<tr>
<td><code>pki</code></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><code>export trustpoint</code></td>
<td>Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key.</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Specify the trustpoint name.</td>
</tr>
<tr>
<td><code>&lt;EXPORT-TO-URL&gt;</code></td>
<td>Specify the destination address in the following format:</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;@&lt;hostname/IP&gt;[:port]//path/file</td>
</tr>
<tr>
<td></td>
<td>http://&lt;hostname/IP&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>cf://path/file</td>
</tr>
<tr>
<td></td>
<td>usb&lt;n&gt;://path/file</td>
</tr>
<tr>
<td><code>background</code></td>
<td>Optional. Performs an export operation in the background</td>
</tr>
<tr>
<td><code>{on &lt;DEVICE-NAME&gt;}</code></td>
<td>on &lt;DEVICE-NAME&gt; – Optional. Performs an export operation on a specified device.</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><code>passphrase</code></td>
<td>Optional. Encrypts the key with a passphrase before exporting</td>
</tr>
<tr>
<td><code>&lt;KEY-PASSPHRASE&gt;</code></td>
<td>&lt;KEY-PASSPHRASE&gt; – Specify the passphrase.</td>
</tr>
<tr>
<td>`{background {on &lt;DEVICE-NAME&gt;}}</td>
<td>background – Optional. Performs export operation in the background</td>
</tr>
<tr>
<td><code>{on &lt;DEVICE-NAME&gt;}</code></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 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>`)}`
```
| Command: crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> | Description: 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 | Description: Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate  
| email <SEND-TO-EMAIL> | Description: Optional. Exports CSR to a specified e-mail address  
| - <SEND-TO-EMAIL> – Specify the CA's e-mail address.  
| fqdn <FQDN> | Description: Optional. Exports CSR to a specified FQDN  
| - <FQDN> – Specify the CA's FQDN.  
| ip-address <IP> | Description: Optional. Exports CSR to a specified device or system  
| - <IP> – Specify the CA's IP address.  
| on <DEVICE-NAME> | Description: Optional. Exports the CSR on a specified device  
| - <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>) } | Description: Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.  
| pki | Description: Generates a self-signed CA certificate and a trustpoint  
| - <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.  
| [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> | Description: 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.  
| subject-name <COMMON-NAME> | Description: Specify a subject name 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.  
| <COUNTRY> | Description: Sets the deployment country code (2 character ISO code)  
| <STATE> | Description: Sets the state name (2 to 64 characters in length)  
| <CITY> | Description: Sets the city name (2 to 64 characters in length)  
| <ORGANIZATION> | Description: Sets the organization name (2 to 64 characters in length)  
| <ORGANIZATION-UNIT> | Description: Sets the organization unit (2 to 64 characters in length)  
| email <SEND-TO-EMAIL> | Description: Optional. Exports the CSR to a specified e-mail address  
| - <SEND-TO-EMAIL> – Specify the CA's e-mail address.  
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto pki import trustpoint &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt;</code></td>
<td>Imports a trustpoint and its associated CA certificate, server certificate, and private key.</td>
</tr>
<tr>
<td><code>&lt;TRUSTPOINT-NAME&gt;</code></td>
<td>Specify the trustpoint name (should be authenticated).</td>
</tr>
</tbody>
</table>
| `<IMPORT-FROM-URL>` | Specify the signed server certificate or CRL source address in the following format:  
  - `tftp://<hostname|IP>[:port]/path/file`
  - `ftp://<user>:<passwd>@<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`
| `background {on <DEVICE-NAME>}` | Optional. Performs import operation in the background. |
| `on <DEVICE-NAME>` | Optional. Performs import operation on a specified device. |
| `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. |
| `[certificate|crl] <TRUSTPOINT-NAME>` | Imports a signed server certificate or CRL. |
| `<TRUSTPOINT-NAME>` | Specify the trustpoint name (should be authenticated). |
| `<IMPORT-FROM-URL>` | Specify the signed server certificate or CRL source address in the following format:  
  - `tftp://<hostname|IP>[:port]/path/file`
  - `ftp://<user>:<passwd>@<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`
| `background {on <DEVICE-NAME>}` | Optional. Performs import operation in the background. |
| `on <DEVICE-NAME>` | Optional. Performs import operation on a specified device. |
| `fqdn <FQDN>` | Optional. Exports the CSR to a specified FQDN. |
| `<FQDN>` | Specify the CA's FQDN. |
| `ip address <IP>` | Optional. Exports the CSR to a specified device or system. |
| `<IP>` | Specify the CA's IP address. |
| `on <DEVICE-NAME>` | Optional. Exports the CSR on a specified device. |
| `<DEVICE-NAME>` | Specify the name of the AP, wireless controller, or service platform. |
| **<IMPORT-FROM-URL>** | Specify the trustpoint source address in the following format:
  - tftp://<hostname>|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<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 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>background</strong>&lt;br&gt;{on &lt;DEVICE-NAME&gt;}</td>
<td>Optional. Performs import operation in the background&lt;br&gt;  - <strong>on &lt;DEVICE-NAME&gt;</strong> – Optional. Performs import operation on a specified device&lt;br&gt;  - <strong>&lt;DEVICE-NAME&gt;</strong> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-NAME&gt;</strong></td>
<td>Optional. Performs import operation on a specified device&lt;br&gt;  - <strong>&lt;DEVICE-NAME&gt;</strong> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td><strong>passphrase</strong>&lt;br&gt;&lt;KEY-PASSPHRASE&gt;&lt;br&gt;{background&lt;br&gt;{on &lt;DEVICE-NAME&gt;}&lt;br&gt;{on &lt;DEVICE-NAME&gt;}}</td>
<td>Optional. Encrypts trustpoint with a passphrase before importing it&lt;br&gt;  - <strong>&lt;KEY-PASSPHRASE&gt;</strong> – Specify a passphrase.&lt;br&gt;  - <strong>background</strong> – Optional. Imports the encrypted trustpoint in the background&lt;br&gt;    - <strong>on &lt;DEVICE-NAME&gt;</strong> – Optional. Imports the encrypted trustpoint on a specified device&lt;br&gt;    - <strong>&lt;DEVICE-NAME&gt;</strong> – 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>}}
  on <DEVICE-NAME>`

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

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

**del-key**<br>{on <DEVICE-NAME>} Optional. Deletes the private key associated with the server certificate<br>  - **on <DEVICE-NAME>** – Optional. Deletes private key on a specified device<br>  - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform. |

**on <DEVICE-NAME>** Optional. Deletes the trustpoint on a specified device<br>  - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform. |

**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><em>no</em></td>
<td>Removes server certificates, trustpoints and their associated certificates</td>
</tr>
</tbody>
</table>
### 3.1.14 delete

*Privileged Exec Mode Commands*

Deletes a specified file from the device's file system

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

**Parameters**

- **/force <FILE>** Forces deletion without a prompt
- **/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#
```
### 3.1.15 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`.

#### Syntax

```bash
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}
device-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
device-upgrade [ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] cancel-upgrade <LOAD-DIRECTORY> [rf-domain]
device-upgrade <MAC/HOSTNAME> [all|ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] cancel-upgrade [mode-reboot-time <TIME>]
device-upgrade cancel-upgrade <MAC/HOSTNAME> [all|ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] all
device-upgrade cancel-upgrade [all|ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] all
device-upgrade load-image <MAC/HOSTNAME> [ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] on
```

#### Supported Platforms

- **Access Points** — AP300, 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, NX9000, NX9500, NX9600, NX9510

#### Syntax

```bash
device-upgrade <MAC/HOSTNAME> [ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] load-image <IMAGE-URL>
device-upgrade rf-domain <RF-DOMAIN-NAME> [ap621|ap622|ap650|ap651|ap652|ap653|ap6562|ap71xx|ap7502|ap7512|ap7522|ap81xx|ap82xx|ap82xx|ap82xx|rf4000|rf5000|rf6000|rf7000|nx45xx|nx50xx|nx75xx|nx9000] all
```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|ap621|ap622|ap650|ap6511|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45XX|nx65XX|nx75XX|nx9000] {<MAC/HOSTNAME>|no-reboot|reboot-time <TIME>} {(staggered-reboot)}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all] [all|ap621|ap622|ap650|ap6511|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45XX|nx65XX|nx75XX|nx9000] {from-controller {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

device-upgrade rf-domain [<RF-DOMAIN-NAME]|all] [all|ap621|ap622|ap650|ap6511|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45XX|nx65XX|nx75XX|nx9000] {upgrade-time <TIME> {no-reboot|reboot-time <TIME>}} {(staggered-reboot)}

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></td>
<td>• &lt;MAC/HOSTNAME&gt; – Specify 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 &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic reboot after a successful upgrade</td>
</tr>
<tr>
<td></td>
<td>• &lt;TIME&gt; – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>upgrade-time &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic device firmware upgrade</td>
</tr>
</tbody>
</table>
|   | • <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. |

- device-upgrade all {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>all</td>
<td>Upgrades firmware on all devices</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 &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic reboot after a successful upgrade</td>
</tr>
<tr>
<td></td>
<td>• &lt;TIME&gt; – Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</td>
</tr>
<tr>
<td>upgrade-time &lt;TIME&gt;</td>
<td>Optional. Schedules an automatic device firmware upgrade on all devices</td>
</tr>
</tbody>
</table>
|   | • <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 common to all of the above. |
|   | • Optional. Enables staggered reboot (one at a time), without network impact |
PRIVILEGED EXEC MODE COMMANDS

- **device-upgrade** [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rf4000|rf6000|rf7000|nx45xx|nx65xx|nx75xx|nx9000] all
  {no-reboot|reboot-time <TIME>|upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}
  {(staggered-reboot)}

Upgrades firmware on all devices of a specific type. Select the device type.

- **AP621 all** – Upgrades firmware on all AP621s
- **AP622 all** – Upgrades firmware on all AP622s
- **AP650 all** – Upgrades firmware on all AP650s
- **AP6511 all** – Upgrades firmware on all AP6511s
- **AP6521 all** – Upgrades firmware on all AP6521s
- **AP6522 all** – Upgrades firmware on all AP6522s
- **AP6532 all** – Upgrades firmware on all AP6532s
- **AP6562 all** – Upgrades firmware on all AP6562s
- **AP71XX all** – Upgrades firmware on all AP71XXs
- **AP7502 all** – Upgrades firmware on all AP7502s
- **AP7522 all** – Upgrades firmware on all AP7522s
- **AP7532 all** – Upgrades firmware on all AP7532s
- **AP81XX all** – Upgrades firmware on all AP81XXs
- **AP82XX all** – Upgrades firmware on all AP82XXs
- **RFS4000 all** – Upgrades firmware on all RFS4000s
- **RFS6000 all** – Upgrades firmware on all RFS6000s
- **RFS7000 all** – Upgrades firmware on all RFS7000s
- **NX45XX all** – Upgrades firmware on all NX45XX series service platforms
- **NX65XX all** – Upgrades firmware on all NX65XX series service platforms
- **NX75XX all** – Upgrades firmware on all NX75XX series service platforms
- **NX9000 all** – Upgrades firmware on all NX9000 series service platforms

After selecting the device type, schedule an automatic upgrade and/or an automatic 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
  - **<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 common to all of the above.
  - **Optional. Enables staggered reboot (one at a time), without network impact**
### device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all]

<table>
<thead>
<tr>
<th>cancel-upgrade</th>
<th>Canceled a scheduled firmware upgrade on a specified device or on all devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>[&lt;MAC/HOSTNAME&gt;</td>
<td>all]</td>
</tr>
<tr>
<td></td>
<td>&lt;MAC/HOSTNAME&gt; keyword. Specify the device’s MAC address or hostname.</td>
</tr>
<tr>
<td></td>
<td>• all – Cancels scheduled upgrade on all devices</td>
</tr>
</tbody>
</table>

### device-upgrade cancel-upgrade [ap621|ap622|ap650|ap651|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] all

<table>
<thead>
<tr>
<th>cancel-upgrade</th>
<th>Canceled scheduled firmware upgrade on all devices of a specific type. Select the device type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ap621</td>
<td>ap622</td>
</tr>
<tr>
<td></td>
<td>• AP622 all – Cancels scheduled upgrade on all AP622s</td>
</tr>
<tr>
<td></td>
<td>• AP650 all – Cancels scheduled upgrade on all AP650s</td>
</tr>
<tr>
<td></td>
<td>• AP651 all – Cancels scheduled upgrade on all AP651s</td>
</tr>
<tr>
<td></td>
<td>• AP6521 all – Cancels scheduled upgrade on all AP6521s</td>
</tr>
<tr>
<td></td>
<td>• AP6522 all – Cancels scheduled upgrade on all AP6522s</td>
</tr>
<tr>
<td></td>
<td>• AP6532 all – Cancels scheduled upgrade on all AP6532s</td>
</tr>
<tr>
<td></td>
<td>• AP6562 all – Cancels scheduled upgrade on all AP6562s</td>
</tr>
<tr>
<td></td>
<td>• AP71XX all – Cancels scheduled upgrade on all AP71XXs</td>
</tr>
<tr>
<td></td>
<td>• AP7502 all – Cancels scheduled upgrade on all AP7502s</td>
</tr>
<tr>
<td></td>
<td>• AP7522 all – Cancels scheduled upgrade on all AP7522s</td>
</tr>
<tr>
<td></td>
<td>• AP7532 all – Cancels scheduled upgrade on all AP7532s</td>
</tr>
<tr>
<td></td>
<td>• AP81XX all – Cancels scheduled upgrade on all AP81XXs</td>
</tr>
<tr>
<td></td>
<td>• AP82XX all – Cancels scheduled upgrade on all AP82XXs</td>
</tr>
<tr>
<td></td>
<td>• RFS4000 all – Cancels scheduled upgrade on all RFS4000s</td>
</tr>
<tr>
<td></td>
<td>• RFS6000 all – Cancels scheduled upgrade on all RFS6000s</td>
</tr>
<tr>
<td></td>
<td>• RFS7000 all – Cancels scheduled upgrade on all RFS7000s</td>
</tr>
<tr>
<td></td>
<td>• NX45XX all – Cancels scheduled upgrade on all NX45XX series service platforms</td>
</tr>
<tr>
<td></td>
<td>• NX65XX all – Cancels scheduled upgrade on all NX65XX series service platforms</td>
</tr>
<tr>
<td></td>
<td>• NX75XX all – Cancels scheduled upgrade on all NX75XX series service platforms</td>
</tr>
<tr>
<td></td>
<td>• NX9000 all – Cancels scheduled upgrade on all NX9000 series service platforms</td>
</tr>
</tbody>
</table>

### device-upgrade cancel-upgrade on rf-domain [<DOMAIN-NAME>|all]

<table>
<thead>
<tr>
<th>cancel-upgrade on rf-domain</th>
<th>Canceled scheduled firmware upgrade in a specified RF Domain or all RF Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>[&lt;RF-DOMAIN-NAME&gt;</td>
<td>all]</td>
</tr>
<tr>
<td></td>
<td>• all – Cancels scheduled device upgrades across all RF Domains</td>
</tr>
</tbody>
</table>
- **device-upgrade load-image**
  - **[ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>load-image</td>
<td>Loads device firmware image from a specified location. Select the device type and provide</td>
</tr>
<tr>
<td></td>
<td>the location of the required device firmware image.</td>
</tr>
<tr>
<td>ap621</td>
<td>Loads AP621 firmware image</td>
</tr>
<tr>
<td>ap622</td>
<td>Loads AP622 firmware image</td>
</tr>
<tr>
<td>ap650</td>
<td>Loads AP650 firmware image</td>
</tr>
<tr>
<td>ap6511</td>
<td>Loads AP6511 firmware image</td>
</tr>
<tr>
<td>ap6521</td>
<td>Loads AP6521 firmware image</td>
</tr>
<tr>
<td>ap6522</td>
<td>Loads AP6522 firmware image</td>
</tr>
<tr>
<td>ap6532</td>
<td>Loads AP6532 firmware image</td>
</tr>
<tr>
<td>ap6562</td>
<td>Loads AP6562 firmware image</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Loads AP71XX firmware image</td>
</tr>
<tr>
<td>ap7502</td>
<td>Loads AP7502 firmware image</td>
</tr>
<tr>
<td>ap7522</td>
<td>Loads AP7522 firmware image</td>
</tr>
<tr>
<td>ap7532</td>
<td>Loads AP7532 firmware image</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Loads AP81XX firmware image</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Loads AP82XX firmware image</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Loads RFS4000 firmware image</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Loads RFS6000 firmware image</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Loads RFS7000 firmware image</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Loads NX45XX series service platform firmware image</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Loads NX65XX series service platform firmware image</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Loads NX75XX series service platform firmware image</td>
</tr>
<tr>
<td>nx9000</td>
<td>Loads NX9000 series service platform firmware image</td>
</tr>
</tbody>
</table>

- **device-upgrade rf-domain**
  - **[<RF-DOMAIN-NAME>|all]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rf-domain</td>
<td>アップグレードスフィアムのデバイスに供給されたRFドメインを含む。RFドメイン内のデバイスはRFドメイン管理者を通じてアップグレードされます。</td>
</tr>
<tr>
<td>&lt;RF-DOMAIN-NAME&gt;</td>
<td>アップグレードデバイスを特定のRFドメインにアップグレードします。RFドメイン名を指定する必要があります。</td>
</tr>
<tr>
<td>all</td>
<td>アップグレードデバイスをすべてのRFドメインにアップグレードします。RFドメイン名を指定する必要があります。</td>
</tr>
</tbody>
</table>

**<IMAGE-URL>** Specify the device’s firmware image location in 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
After specifying the RF Domain, select the device type.

- **all** – Upgrades firmware on all devices
- **AP621** – Upgrades firmware on all AP621s
- **AP622** – Upgrades firmware on all AP622s
- **AP650** – Upgrades firmware on all AP650s
- **AP6511** – Upgrades firmware on all AP6511s
- **AP6521** – Upgrades firmware on all AP6521s
- **AP6522** – Upgrades firmware on all AP6522s
- **AP6532** – Upgrades firmware on all AP6532s
- **AP6562** – Upgrades firmware on all AP6562s
- **AP71XX** – Upgrades firmware on all AP71XXs
- **AP7502** – Upgrades firmware on all AP7502s
- **AP7522** – Upgrades firmware on all AP7522s
- **AP7532** – Upgrades firmware on all AP7532s
- **AP81XX** – Upgrades firmware on all AP81XXs
- **AP82XX** – Upgrades firmware on all AP82XXs
- **RFS4000** – Upgrades firmware on all RFS4000s
- **RFS6000** – Upgrades firmware on all RFS6000s
- **RFS7000** – Upgrades firmware on all RFS7000s
- **NX45XX** – Upgrades firmware on all NX45XX series service platforms
- **NX65XX** – Upgrades firmware on all NX65XX series service platforms
- **NX75XX** – Upgrades firmware on all NX75XX series service platforms
- **NX9000** – Upgrades firmware on all NX9000 series service platforms

| `<MAC/HOSTNAME>` | Optional. Upgrades firmware on the device identified by the `<MAC/HOSTNAME>` keyword. 
| `<MAC/HOSTNAME>` | – Specify the device’s MAC address or hostname. |
| `no-reboot` | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted). |
| `{staggered-reboot}` | |
| `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}` | |
| `staggered-reboot` | This keyword is common to all of the above. 
| | Optional. Enables staggered reboot (one at a time), without network impact |

- `device-upgrade rf-domain [RF-DOMAIN-NAME]|all] [all|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] [from-controller {no-reboot|reboot-time <TIME>} {staggered-reboot}]` |

- `rf-domain [RF-DOMAIN-NAME]|all]` | Upgrades firmware on devices in a specified RF Domain or all RF Domains |
| `<RF-DOMAIN-NAME>` | – Upgrades devices in a specified RF Domain. Specify the RF Domain name. |
| `all` | – Upgrades devices across all RF Domains |
After specifying the RF Domain, select the device type:

- **all** – Upgrades firmware on all devices
- **AP621** – Upgrades firmware on all AP621s
- **AP622** – Upgrades firmware on all AP622s
- **AP650** – Upgrades firmware on all AP650s
- **AP6511** – Upgrades firmware on all AP6511s
- **AP6521** – Upgrades firmware on all AP6521s
- **AP6522** – Upgrades firmware on all AP6522s
- **AP6532** – Upgrades firmware on all AP6532s
- **AP6562** – Upgrades firmware on all AP6562s
- **AP71XX** – Upgrades firmware on all AP71XXs
- **AP7502** – Upgrades firmware on all AP7502s
- **AP7522** – Upgrades firmware on all AP7522s
- **AP7532** – Upgrades firmware on all AP7532s
- **AP81XX** – Upgrades firmware on all AP81XXs
- **AP82XX** – Upgrades firmware on all AP82XXs
- **RFS4000** – Upgrades firmware on all RFS4000s
- **RFS6000** – Upgrades firmware on all RFS6000s
- **RFS7000** – Upgrades firmware on all RFS7000s
- **NX45XX** – Upgrades firmware on all NX45XX series service platforms
- **NX65XX** – Upgrades firmware on all NX65XX series service platforms
- **NX75XX** – Upgrades firmware on all NX75XX series service platforms
- **NX9000** – Upgrades firmware on all NX9000 series service platforms

**from-controller**
Optional. Upgrades a device through the adopted device

**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.

**upgrade-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.

**staggered-reboot**
This keyword is common to all of the above.
Optional. Enables staggered reboot (one at a time), without network impact
### device-upgrade rf-domain

- **rf-domain [<RF-DOMAIN-NAME>|all]**
  - **[<RF-DOMAIN-NAME>|all]**
    - **<RF-DOMAIN-NAME>** – Upgrades devices in a specified RF Domain. Specify the RF Domain name.
    - **all** – Upgrades devices across all RF Domains

- **upgrade <TIME>**
  - Optional. Schedules an automatic device firmware upgrade.
    - **<TIME>** – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format.

- **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>NX7500</th>
<th>NX9000</th>
<th>NX9XXX (NX9500 &amp; NX9510)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS4000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RFS6000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RFS7000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX45XX</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NX65XX</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX7500</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NX9000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>NX9XXX</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

NOTE: The NX7500 series service platform supports HM networks. At the lower end, it replaces RFS7000, and at the upper end it is adopted by NX9500. A NX7500 adopted by a NX9500 is the common deployment pattern used for the NX7500 series service platform.

Examples

rfs4000-229D58#device-upgrade rfs4000-229D58 no-reboot
rfs4000-229D58#

rfs4000-229D58#show device-upgrade ?
history History of Device Upgrade
load-image-status Status of firmware file download on the device
status Status of Device Upgrade
versions Versions of device-upgrade images

rfs4000-229D58#show device-upgrade
rfs4000-229D58#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>ap71xx-0F43D8</td>
<td>failed</td>
<td>2014-01-05 00:21:08</td>
<td>3</td>
<td>00-23-68-22-9D-58</td>
<td>Update error: Unable to get update file, failure in ftp/openssl/tar</td>
</tr>
<tr>
<td>ap6532-986C50</td>
<td>failed</td>
<td>2014-01-05 00:26:31</td>
<td>3</td>
<td>00-23-68-22-9D-58</td>
<td>Update error: Bad file, failure in tar. tar: invalid tar magic</td>
</tr>
</tbody>
</table>

Total number of entries displayed: 2

rfs4000-229D58#
rfs4000-229D58#show device-upgrade versions

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>DEVICE-TYPE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfs4000-229D58</td>
<td>ap621</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap622</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap650</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6511</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6521</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6522</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6532</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap6562</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap71xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap81xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>ap82xx</td>
<td>none</td>
</tr>
<tr>
<td>rfs4000-229D58</td>
<td>rfs4000</td>
<td>none</td>
</tr>
</tbody>
</table>

rfs4000-229D58#
3.16 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5700, NX5724, NX7500, NX9000, NX9500, NX9600, NX9510

Syntax

diff [<FILE>|<URL>] [<FILE>|<URL>]

Parameters

- diff [<FILE>|<URL>] [<FILE>|<URL>]

Examples

rfs4000-229D58#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
+! Configuration of RFS4000 version 5.5.6.0-006D
+
+!@@ -779,13 +780,11 @@
+ alias vlan $testVLANAlias 1
!
 rfs4000 00-23-68-22-9D-58
 - radio-count 0
 - use profile default-rfs4000
 - use rf-domain default
 hostame rfs4000-229D58
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 - adoption-site Test-EcoSpace3B
 - mint mlcp vlan
 - mint mlcp ip
 - wep-shared-key-auth

rfs4000-229D58#
3.1.17 `dir`

Privileged Exec Mode Commands

Lists files on a device’s file system

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

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

```
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# dir all-filesystems
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
```

```
Directory of nvram:/.
  -rw-  10669   Sat Jan 14 02:47:11 2014   startup-config.save
```

```
Directory of system:/.
  drwx       Wed Jan 16 22:35:18 2014   proc
rfs4000-229D58#
```
3.1.18 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

disable

**Parameters**

None

**Examples**

rfs7000-37FABE#disable
rfs7000-37FABE>
3.1.19 edit

Privileged Exec Mode Commands

Edits a text file on the device’s file system

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax
edit <FILE>

Parameters

- edit <FILE>

| <FILE> | Specify the name of the file to modify. |

Examples

rfs4000-229D58#edit startup-config
GNU nano 1.2.4                File: startup-config

! Configuration of RFS4000 version 5.5.6.0-006D
!
!
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%) ]
3.1.20 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

```
enable
```

Parameters

None

Examples

```
rfs7000-37FABE#enable
rfs7000-37FABE#
```
3.1.21 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

Syntax
erase [cf:|flash:|nvram:|startup-config|usb1:]

Parameters
- erase [cf:|flash:|nvram:|startup-config|usb1:]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cf:</td>
<td>Erases everything in the device’s cf: file</td>
</tr>
<tr>
<td>flash:</td>
<td>Erases everything in the device’s flash: file</td>
</tr>
<tr>
<td>nvram:</td>
<td>Erases everything in the device’s nvram: file</td>
</tr>
<tr>
<td>startup-config</td>
<td>Erases the device’s startup configuration file. The startup configuration file is used to configure the device when it reboots.</td>
</tr>
<tr>
<td>usb1:</td>
<td>Erases everything in the device’s usb1: file</td>
</tr>
</tbody>
</table>

Examples
rfs7000-37FABE#erase startup-config
Erase startup-config? (y/n): n
rfs7000-37FABE#
### 3.1.22 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

#### Syntax

```
halt {on <DEVICE-NAME>}
```

#### Parameters

- `halt {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>halt</code></td>
<td>Halts a specified device</td>
</tr>
<tr>
<td><code>{on &lt;DEVICE-NAME&gt;}</code></td>
<td>Optional. Enter the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**Note:** If the device name is not specified, the logged device is halted.

#### Examples

```
rfs7000-37FABE# halt on rfs7000-37FABE
rfs7000-37FABE#
```
3.1.23 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

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>join-cluster</td>
<td>Adds a access point, wireless controller, or service platform to an existing cluster</td>
</tr>
<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></td>
<td>• 1 – Configures level 1 routing</td>
</tr>
<tr>
<td></td>
<td>• 2 – Configures level 2 routing</td>
</tr>
<tr>
<td>mode [active</td>
<td>standby]</td>
</tr>
<tr>
<td></td>
<td>• active – Configures cluster mode as active</td>
</tr>
<tr>
<td></td>
<td>• standby – Configures cluster mode as 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 172.16.10.10 user admin password example
Joining cluster at 172.16.10.10... Done
Please execute “write memory” to save cluster configuration.

rfs7000-37FABE#

nx6500-31FABE#join-cluster 172.16.10.10 user admin password example
Joining cluster at 172.16.10.10... Done
Please execute “write memory” to save cluster configuration.

nx6500-31FABE#

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>
### 3.1.24 l2tpv3

**Privileged Exec Mode Commands**

Establishes or brings down an L2TPv3 tunnel

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```plaintext
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>}`
  
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2tpv3 tunnel &lt;TUNNEL-NAME&gt; [down</td>
<td>up] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>&lt;TUNNEL-NAME&gt; — Specify the tunnel name.</td>
<td></td>
</tr>
<tr>
<td>down — Brings down the specified tunnel</td>
<td></td>
</tr>
<tr>
<td>up — Establishes the specified tunnel</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; — Optional. Establishes or brings down a tunnel 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>

- `l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}`
  
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2tpv3 tunnel &lt;TUNNEL-NAME&gt; session &lt;SESSION-NAME&gt; [down</td>
<td>up] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>&lt;TUNNEL-NAME&gt; — Specify the tunnel name.</td>
<td></td>
</tr>
<tr>
<td>session &lt;SESSION-NAME&gt; — Specify the session name.</td>
<td></td>
</tr>
<tr>
<td>down — Brings down the specified tunnel session</td>
<td></td>
</tr>
<tr>
<td>up — Establishes the specified tunnel session</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; — Optional. Establishes or brings down a tunnel session 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>

- `l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}`
  
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2tpv3 tunnel all [down</td>
<td>up] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>down — Brings down all tunnels</td>
<td></td>
</tr>
<tr>
<td>up — Establishes all tunnels</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; — Optional. Establishes or brings down all tunnels 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
rfs7000-37FABE#l2tpv3 tunnel Tunnell session TunnelSession1 up on rfs7000-37FABE

NOTE: For more information on the L2TPv3 tunnel configuration mode and commands, see Chapter 23, L2TPV3-POLICY.
### 3.1.25 logging

- **Privileged Exec Mode Commands**

Modifies message logging settings

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>monitor</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;0-7&gt;</code> – Optional. Enter the logging severity level from 0 - 7. The various levels and their implications are:</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>

**Examples**

```
rfs7000-37FABE#logging monitor warnings
rfs7000-37FABE#
```

```
rfs7000-37FABE#logging monitor 2
rfs7000-37FABE#
```

**Related Commands**

- `no` Resets terminal lines logging levels
### 3.1.26 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```plaintext
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**

- **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 - 60. The default is 3.

- **size <1-64000>**
  
  Optional. Sets the MiNT payload size in bytes
  - `<1-64000>` — Specify a value from 1 - 640000 bytes. The default is 64 bytes.

- **timeout <1-10>**
  
  Optional. Sets a response time in seconds
  - `<1-10>` — Specify a value from 1 - 10 seconds. 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
  - `<1-255>` — Specify a value from 1 - 255 seconds. The default is 30 seconds.
Examples

rfs7000-37FABE#mint ping 68.22.9B.58 count 6 size 128
MiNT ping 68.22.9B.58 with 128 bytes of data.
Ping request 1 timed out. No response from 68.22.9B.58
Ping request 2 timed out. No response from 68.22.9B.58
Ping request 3 timed out. No response from 68.22.9B.58
Ping request 4 timed out. No response from 68.22.9B.58
Ping request 5 timed out. No response from 68.22.9B.58
Ping request 6 timed out. No response from 68.22.9B.58

--- 68.22.9B.58 ping statistics ---
6 packets transmitted, 0 packets received, 100% packet loss
rfs7000-37FABE#
3.1.27 mkdir

*Privileged Exec Mode Commands*

Creates a new directory in the file system

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```shell
mkdir <DIR>
```

**Parameters**

- `mkdir <DIR>`

<table>
<thead>
<tr>
<th><code>&lt;DIR&gt;</code></th>
<th>Specify a directory name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> A directory, specified by the <code>&lt;DIR&gt;</code> parameter, is created within the file system.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```shell
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#
```

```shell
rfs4000-229D58#mkdir testdir
rfs4000-229D58#
```

```shell
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#
```
3.1.28 more

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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

`more <FILE>`

Parameters

- `more <FILE>`

Examples

```
more flash:/log/messages.log
Jan 01 00:04:12 2014: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'admin' from 'ssh'
Jan 01 02:06:53 2014: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'admin(superuser)' from 'ssh'
Jan 01 02:07:01 2014: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'admin(superuser)' from 'ssh'
Jan 01 02:23:26 2014: rfs4000-229D58 : %NSM-4-IFDOWN: Interface ge1 is down
Jan 01 02:24:25 2014: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
Jan 01 02:24:26 2014: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
Jan 01 02:24:33 2014: rfs4000-229D58 : %NSM-4-IFDOWN: Interface ge1 is down
Jan 01 02:24:40 2014: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
Jan 01 02:24:40 2014: rfs4000-229D58 : %NSM-4-IFUP: Interface ge1 is up
```

```
rfs4000-229D58#
```
### 3.1.29 no

**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** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```bash
no [adoption|captive-portal|crypto|debug|logging|mac-user-db|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]
no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>} on <DEVICE-NAME>}

no logging monitor

no page

no service [ap300|block-adopter-config-update|locator|ssm|wireless]
no service ap300 locator <MAC>
no service block-adopter-config-update
no service locator {on <DEVICE-NAME>}
no service [ssm|wireless] trace pattern {<WORD>|on <DEVICE-NAME>}

no terminal [length|width]

no upgrade <PATCH-NAME> {on <DEVICE-NAME>}

no wireless client [all|<MAC>]
no wireless client all {filter|on}
no wireless client all {filter [wlan <WLAN-NAME>]}{filter [wlan <WLAN-NAME>]}
no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-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 mac-user-db user [<USER-NAME>|all]
no raid locate
### Parameters

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

  Resets adoption status of a specified device or all devices in a specified RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` – Optional. Enter the name of the AP, wireless controller, service platform, or RF Domain. This command resets the adoption status of the specified device and all devices adopted by it.

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

  Disconnects captive portal clients from the network
  - `<CAPTIVE-PORTAL-NAME>` – Specify the captive portal name.
  - `<MAC>` – Specify the client’s MAC address.
  - `<DEVICE-OR-DOMAIN-NAME>` – Optional. Disconnects a specified captive portal client or all clients on a specified device or RF Domain.

- **no crypto pki {server|trustpoint} <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}}{on <DEVICE-OR-DOMAIN-NAME>}

  Deletes all PKI authentications
  - `<TRUSTPOINT-NAME>` – Deletes a trustpoint or its server certificate. Specify the trustpoint name.
  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

  The following keyword is common to the server and trustpoint parameters:
  - `<TRUSTPOINT-NAME>` – Deletes a trustpoint or its server certificate. Specify the trustpoint name.

- **no logging monitor

  Resets terminal lines message logging levels

- **no page

  Resets controller paging function to its default. Disabling the “page” command displays the CLI command output at once, instead of page by page.
- **no service ap300 locator <MAC>**

  Disables LEDs on AP300s or a specified device in the WLAN. It also resets the CLI table and MiNT protocol configurations.

  - **ap300 locator <MAC>**
    - Disables LEDs on AP300s
      - <MAC> – Specify the AP300’s MAC address.

- **no service block-adopter-config-update**

  Enables configuration updates from the NOC controller. If the configuration update from the NOC controller feature is blocked, use the `no service block-adopter-config-update` command to enable it.

- **no service locator {on <DEVICE-NAME>]**

  Disables LEDs on a specified device in the WLAN. It also resets the CLI table expand and MiNT protocol configurations.

  - **locator {on <DEVICE-NAME>]**
    - Disables LEDs on a specified device
      - <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform.

- **no service [ssm|wireless] trace pattern {<WORD>|on <DEVICE-NAME>}**

  Disables certain specified services or features

  - **[ssm|traceroute]**
    - Disables the following features:
      - ssm – Disables Security Services Module (SSM) related services
      - traceroute – Disables wireless related services
    - **trace**
      - The following command is common to the ‘ssm’ and ‘wireless’ parameters:
        - trace – Traces SSM or wireless related services
    - **pattern {<WORD>|on <DEVICE-NAME>**
      - Configures the pattern to match
        - <WORD> – Optional. Specify the pattern to ignore. Reverses the match pattern specified.
        - on <DEVICE-NAME> – Optional. Matches the specified pattern on specified device.
        - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

- **no upgrade <PATCH-NAME> {on <DEVICE-NAME>**

  Removes a patch installed on a specified device

  - **no upgrade <PATCH-NAME>**
    - Removes a patch installed on a specified device
      - <PATCH-NAME> – Specify the name of the patch.
  - **on <DEVICE-NAME>**
    - Optional. Removes a patch on a specified device
      - <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
- **no terminal [length|width]**

  *no terminal [length|width]*  
  Resets the width of the terminal window, or the number of lines displayed within the terminal window
  - *length* – Resets the number of lines displayed on the terminal window to its default
  - *width* – Resets the width of the terminal window to its default.

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

  *no wireless client all*  
  Disassociates all wireless clients on a specified device or domain

  *filter wlan <WLAN-NAME>*  
  Optional. Specifies an additional client selection filter
  - *wlan* – Filters clients on a specified WLAN
  - *<WLAN-NAME>* – Specify the WLAN name.

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

  *no wireless client all*  
  Disassociates all clients on a specified device or domain

  *on <DEVICE-OR-DOMAIN-NAME>*  
  Optional. Specifies the name of the AP, wireless controller, service platform, or RF Domain.

  *filter [wlan <WLAN-NAME>]*  
  Optional. Specifies an additional client selection filter
  - *wlan* – Filters clients on a specified WLAN
  - *<WLAN-NAME>* – Specify the WLAN name.

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

  *no wireless client mac <MAC>*  
  Disassociates a single wireless client on a specified device or RF Domain

  *on <DEVICE-OR-DOMAIN-NAME>*  
  Optional. Specifies the name of the AP, wireless controller, service platform, or RF Domain to which the specified client is associated

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

  *no virtual-machine assign-usb-ports*  
  Reverts ports assigned for virtual-machines back to WiNG

  **Note:** This command is available only on the NX45XX, NX65XX, NX9500, and NX9510 series service platforms.

  *on <DEVICE-NAME>*  
  Reverts virtual-machine assigned ports on a specified device

  *on <DEVICE-NAME>*  
  Optional. Specify the name of the AP, wireless controller, or service platform.

- **no mac-user-db user [<USER-NAME>|all]**

  *no mac-user-db user*  
  Deletes a specified user or all users from the MAC registration user database

  **Note:** This command is available only on the NX9000 series service platforms.

  *<USER-NAME>*  
  Deletes the user, identified by the *<USER-NAME>* keyword, from the MAC registration user database

  *<USER-NAME>*  
  – Specify the username.

  *all*  
  Deletes all users from the MAC registration user database
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#

rfs7000-37FABE# no service cli-tables-expand line
rfs7000-37FABE#

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-provisioning-policy</td>
<td>Resets the adoption state of a device and all devices adopted to it</td>
</tr>
<tr>
<td>captive portal</td>
<td>Manages captive portal clients</td>
</tr>
<tr>
<td>crypto</td>
<td>Enables digital certificate configuration and RSA Keypair management</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging settings</td>
</tr>
<tr>
<td>page</td>
<td>Resets controller paging function to its default</td>
</tr>
<tr>
<td>service</td>
<td>Performs different functions depending on the parameter passed</td>
</tr>
<tr>
<td>terminal</td>
<td>Sets the length or the number of lines displayed within the terminal window</td>
</tr>
<tr>
<td>upgrade</td>
<td>Upgrades software image on a device</td>
</tr>
<tr>
<td>wireless-client</td>
<td>Manages wireless clients</td>
</tr>
<tr>
<td>virtual-machine</td>
<td>Installs, configures, and monitors the status of third-party VMs</td>
</tr>
<tr>
<td>raid</td>
<td>Enables Redundant Array of Independent Disks (RAID) management</td>
</tr>
</tbody>
</table>
Privileged Exec Mode Commands

3.1.30 page

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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

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>
3.1.31 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>}
```

**Parameters**
- `ping <IP/HOSTNAME>`
  - `{count <1-10000>|dont-fragment {count|size}|size <1-64000>}`
  - `<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.

**Examples**
```bash
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#
```
### 3.1.32 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** — AP300, 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, NX9000, NX9500, NX9600, NX9510

#### Syntax

```plaintext
pwd
```

#### Parameters

None

#### Examples

```plaintext
rfs4000-229D58#pwd
flash:/
rfs4000-229D58#

rfs4000-229D58#dir
Directory of flash:/.

drwx Wed Jan 30 02:45:10 2014 log

```

rfs4000-229D58#```
3.1.33 **re-elect**

Privileged Exec Mode Commands

Re-elects the tunnel controller (wireless controller or service platform)

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
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>
<tbody>
<tr>
<td>&lt;WORD&gt; {on &lt;DEVICE-NAME&gt;}</td>
<td>Optional. Re-elects the tunnel controller on all devices whose preferred tunnel controller name matches &lt;WORD&gt;</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt; — Optional. Re-elects the tunnel controller 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**

```
rfs7000-37FABE#re-elect tunnel-controller
OK
rfs7000-37FABE#
```
### 3.1.34 reload

**Privileged Exec Mode Commands**

Halts the device and performs a warm reboot

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
reload {cancel|force|in|on} 
reload {on <DEVICE-OR-DOMAIN-NAME>} 
reload {cancel|force} {on <DEVICE-OR-DOMAIN-NAME>} 
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>} 
```

**Parameters**
- **reload {on <DEVICE-OR-DOMAIN-NAME>}**
  
  Optional. Performs reload on a specified device or RF Domain. Halts the system and performs a warm reboot
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- **reload {cancel|force} {on <DEVICE-OR-DOMAIN-NAME>}**
  
  Optional. Cancels or forces a reload on a specified device or RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.

- **cancel**
  
  Optional. Cancels pending reloads

- **force**
  
  Optional. Forces reboot, while ignoring conditions like upgrade in progress, unsaved changes etc.

- **on <DEVICE-OR-DOMAIN-NAME>**
  
  Optional. Performs a reload after a specified time period
  - `<1-999>` – Specify the time from 1 - 999 minutes.

- **list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}**
  
  Optional. Reloads all adopted devices or specified devices
  - `<LINE>` – Optional. Reloads listed devices. List all devices (to be reloaded) separated by a space.
  - `all` – Optional. Reloads all devices adopted by this controller

- **on <DEVICE-OR-DOMAIN-NAME>**
  
  Optional. Reloads on a specified device or RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.

**Examples**

```
rfs7000-37FABE#reload force on rfs7000-37FABE
rfs7000-37FABE#
```
3.1.35 rename

Privileged Exec Mode Commands

Renames a file in the devices’ file system

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

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 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 crashinfo
drwx Wed Jan 16 22:26:53 2014 archived_logs
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#
### 3.1.36 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6532, NX7500, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
rmdir <DIR>
```

**Parameters**

- **rmdir <DIR>**

**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   archived_logs
  drwx    Sat Jan 1  00:00:09 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   archived_logs
  drwx    Sat Jan 1  00:00:09 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#
```
3.1.37 self

Privileged Exec Mode Commands

Enters the logged device’s configuration context

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

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)#
3.1.38 ssh

*Privileged Exec Mode Commands*

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

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
ssh <IP/HOSTNAME> <USERNAME>
```

**Parameters**

- `ssh <IP/HOSTNAME> <USERNAME>`

<table>
<thead>
<tr>
<th>&lt;IP/HOSTNAME&gt;</th>
<th>Specify the remote system's IP address or hostname.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify the name of the user requesting the SSH connection.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To exit the other device’s context, use the command that is relevant to that device.

**Examples**

```
rfs7000-37FABE#ssh 172.16.10.8 admin
admin@172.16.10.8's password:
rfs4000-229D58>
```
3.1.39 **telnet**

*Privileged Exec Mode Commands*

Opens a Telnet session between two network devices

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532,
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

**Syntax**

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

**Parameters**

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

<table>
<thead>
<tr>
<th>&lt;IP/HOSTNAME&gt;</th>
<th>Configures the remote system’s IP address or hostname. The Telnet session is established between the connecting system and the remote system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;IP&gt; — Specify the remote system’s IP address or hostname.</td>
</tr>
</tbody>
</table>

| <TCP-PORT>                  | Optional. Specify the Transmission Control Protocol (TCP) port. |

**Usage Guidelines**

To exit the other device’s context, use the command relevant to that device.

**Examples**

rfs4000-229D58#telnet 192.168.13.23

Entering character mode
Escape character is ‘^]’.

AP7131 release 5.5.6.0-006D
ap7131-11B6C4 login: admin
Password:
ap7131-11B6C4>
### 3.1.40 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532,
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX7550, NX9000, NX9500, NX9600, NX9510

**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 &lt;0-512&gt;</td>
<td>Sets the number of lines displayed on a terminal window. This value is limited to a maximum of 512.</td>
</tr>
<tr>
<td>width &lt;0-512&gt;</td>
<td>Sets the width or number of characters displayed on the terminal window. This value is limited to a maximum of 512.</td>
</tr>
</tbody>
</table>

**Examples**
```
rfs7000-37FABE#terminal length 150
rfs7000-37FABE#
rfs7000-37FABE#terminal width 215
rfs7000-37FABE#
```

**Related Commands**
- no

Resets the width of the terminal window or the number of lines displayed on a terminal window.
3.1.41 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

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)#
### 3.1.42 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

`traceroute <LINE>`

**Parameters**

- `traceroute <LINE>`

<table>
<thead>
<tr>
<th>&lt;LINE&gt;</th>
<th>Traces the route to a destination IP address or hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;LINE&gt;</code> — Specify a traceroute argument. For example, “service traceroute-h”.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE# traceroute 172.16.10.2
traceroute to 172.16.10.2 (172.16.10.2), 30 hops max, 38 byte packets
  1  172.16.10.1 (172.16.10.1) 3002.008 ms !H  3002.219 ms !H  3003.945 ms !H
rfs7000-37FABE#
```
3.1.43 upgrade

Privileged Exec Mode Commands

Upgrades a device’s software image.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>}

Parameters

- upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FILE&gt;</td>
<td>Specify the target firmware image location in the following format:</td>
</tr>
<tr>
<td></td>
<td>cf:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb1:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb2:/path/file</td>
</tr>
<tr>
<td>&lt;URL&gt;</td>
<td>Specify the target firmware image location in the following format:</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;</td>
</tr>
<tr>
<td></td>
<td>http://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>cf:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb&lt;n&gt;:/path/file</td>
</tr>
<tr>
<td>background</td>
<td>Optional. Performs upgrade in the background</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Upgrades the software image on a specified remote 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#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

rfs7000-37FABE#upgrade tftp://157.125.208.235/img
Running from partition /dev/mtdblock7, partition to update is /dev/mtdblock6

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>
3.1.44 **upgrade-abort**

- Privileged Exec Mode Commands

Aborts an ongoing software image upgrade

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**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><code>upgrade-abort</code></td>
<td>Aborts an ongoing software image upgrade</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>Optional. Aborts an ongoing software image upgrade 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**

```
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W551/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/W551/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#
```
3.1.45 watch

Repeats a specified CLI command at periodic intervals

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX7500, NX9500, NX9600, NX9510

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#
3.1.46 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

Syntax

exit

Parameters

None

Examples

rfs7000-37FABE#exit
3.1.47 **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 `url-list`.

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

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

**Parameters**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smart-cache</td>
<td>Pre-fetches content from the specified list of URLs</td>
</tr>
<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 <code>url-list</code>.</td>
</tr>
</tbody>
</table>

**Examples**

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

nx4500-5CFA2B#
```
3.1.48 virtual-machine

Privileged Exec Mode Commands

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

In addition to the shipped VMs, the NX45XX, NX65XX, NX9500, NX9600, 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 are:

- 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

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9500, NX9510

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]|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]


vif-count <0-2>|vif-mac <VIF-INDEX>|vif-to-vmif <VMIF-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]|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}

virtual-machine stop hard [<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**
- `virtual-machine assign-usb-ports team-vowlan [on <DEVICE-NAME>]`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assign-usb-ports</td>
<td>Assigns USB ports to TEAM-VoWLAN on a specified device</td>
</tr>
<tr>
<td>team-vowlan</td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Specify the device name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use the <code>no &gt; virtual-machine &gt; assign-usb-ports</code> to reassign the port to WiNG.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-machine console</td>
<td>Connects to the VM’s console, based on the parameters passed. Select one of the following console options:</td>
</tr>
<tr>
<td>&lt;VM-NAME&gt;</td>
<td>• &lt;VM-NAME&gt; – Connects to the console of the VM identified by the &lt;VM-NAME&gt; keyword. Specify the VM name.</td>
</tr>
<tr>
<td>team-urc</td>
<td>• team-urc – Connects to the VM TEAM-URC’s (IP-PBX) console</td>
</tr>
<tr>
<td>team-rls</td>
<td>• team-rls – Connects to the VM TEAM Radio Link Server’s (RLS) console</td>
</tr>
<tr>
<td>team-vowlan</td>
<td>• team-vowlan – Connects to the VM TEAM-VoWLAN’s (Voice over WLAN) console</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-machine export</td>
<td>Exports an existing VM image and settings. Use this command to export the VM to another NX45XX or NX65XX device in the same domain.</td>
</tr>
<tr>
<td>&lt;VM-NAME&gt;</td>
<td>• Specify the VM name.</td>
</tr>
<tr>
<td>&lt;FILE&gt;</td>
<td>• Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.</td>
</tr>
<tr>
<td>&lt;URL&gt;</td>
<td>• 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:</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname&gt;[:port]/path/file</td>
</tr>
<tr>
<td></td>
<td>http://&lt;hostname&gt;[:port]/path/file</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Executes the command on a specified device or devices</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the service platform name. In case of multiple devices, list the device names separated by commas.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The VM should be in a stop state during the export process.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If the destination is a device, the image is copied to a predefined location (VM archive)</td>
</tr>
</tbody>
</table>
### 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}*  

**virtual-machine install** 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).
  - **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, or tftp.

<table>
<thead>
<tr>
<th>install-media</th>
<th>Specifies the install media location</th>
</tr>
</thead>
</table>
| [<FILE>|<URL>|<USB>] | - **<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.

Contd...
### virtual-machine install

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.

#### Parameters

- **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 or disables 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 restart

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.

**Note:** 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>|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>|vnc [disable|enable]] [{on <DEVICE-NAME>}]
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

**virtual-machine start**

Starts the VM, based on the parameters passed. Select one of the following options:

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

**virtual-machine stop**

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.

**Note**: The option ‘hard’ forces the selected VM to shutdown

**virtual-machine uninstall**

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

```plaintext
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 NX9XXX, 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 NX9XXX series service platform.

---

**Parameters NX9500 and NX9510**

- `virtual-machine console adsp`

  `virtual-machine console` Connects to the Air-Defense Services Platform (ADSP) VM's 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>}

**virtual-machine install**

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.

**Note:** 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:

```
nx9500-6C874D#upgrade tftp://20.1.1.60/adsp-9.1.1Aug 20
15:12:41 2014: %DAEMON-6-INFO: lighttpd[2405]: 127.0.0.1
127.0.0.1:443 - "POST /mapi.fcgi HTTP/1.1" 200 192 "-" "-"
-03-5.5.6.0-006D.img
Aug 20 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)......Aug 20
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>}

**virtual-machine restart**

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 <DEVICE-NAME>}

**virtual-machine set disk-size**

Sets the ADSP VM’s disk size (in GB). Specify a value from 100 - 500 GB.

- **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:** Stop the ADSP VM before executing this command.

- virtual-machine set memory <512-8192> adsp {on <DEVICE-NAME>}

**virtual-machine set memory**

Modifies the ADSP VM’s memory. Specify a value from 512 - 8192 MB.

- **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

  **Note:** 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.

  **Note:** 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

  • 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 > [configuration|debugging|export|statistics] command to view installed VM details.
3.1.49 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 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 — NX9500, NX9600, NX7500

**NOTE:** The NX9500 service platform includes a single Intel MegaRAID controller, configured to provide a single virtual drive. This virtual drive is of the RAID-1 type, and has a maximum of two physical drives. In addition to these two drives, there are three hot spares, which are used in case of a primary drive failure.

**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.

  **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`.

- **raid [install|locate|remove|spare] drive <0-4>**

  **install <0-4>**
  Includes a new drive, inserted in one of the available slots, in the array. Specify the drive number.
  - **Note:** Drives 0 and 1 are the array drives. Drives 2, 3, and 4 are the hot spare drives. You can include the new drive in a degraded array, or enable it as a hot spare.
  - **Note:** If the array is in a degraded state, the re-build process is triggered and the new drive is used to repair the degraded array.

  **locate <0-4>**
  Enables LEDs to blink on a specified drive. Specify the drive number.
  - **Note:** Blinking LEDs enable you correctly locate a drive.

  **remove <0-4>**
  Removes (shuts downs) a disk from the array, before it is physically removed from its slot. Specify the drive number containing the disk.
  - **Note:** Use this command to also remove a hot spare.

  **spare <0-4>**
  Converts an unused drive into a hot spare. Specify the drive number.

### Examples

```
nx9500-6C874D#raid install drive 0
Error: Input Error: Drive 0 is already member of array, can't be added
nx9500-6C874D#

nx9500-6C8809*#raid spare drive 1
Error: RAID operation failed, returned 2, output: Input Error: Drive 1 is member of array, can't be a hotspare
/
nx9500-6C8809*#
```
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 privileged 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
- aaa-tacacs-policy
- alias
- ap300
- ap621
- ap622
- ap650
- ap6511
- ap6521
- ap6522
- ap6532
- ap6562

Configure authentication/accounting/authorization
Configure an authentication/accounting/authorization TACACS policy
Alias
Configure an AP300
AP621 access point
AP622 access point
AP650 access point
AP6511 access point
AP6521 access point
AP6522 access point
AP6532 access point
AP6562 access point
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap7502</td>
<td>AP7502 access point</td>
</tr>
<tr>
<td>ap7522</td>
<td>AP7502 access point</td>
</tr>
<tr>
<td>ap7532</td>
<td>AP7532 access point</td>
</tr>
<tr>
<td>ap71xx</td>
<td>AP71XX access point</td>
</tr>
<tr>
<td>ap81xx</td>
<td>AP81XX access point</td>
</tr>
<tr>
<td>ap82xx</td>
<td>AP82XX access point</td>
</tr>
<tr>
<td>association-acl-policy</td>
<td>Configure an association acl policy</td>
</tr>
<tr>
<td>auto-provisioning-policy</td>
<td>Configure an auto-provisioning policy</td>
</tr>
<tr>
<td>bonjour-gw-discovery-policy</td>
<td>Bonjour Gateway discovery policy</td>
</tr>
<tr>
<td>bonjour-gw-forwarding-policy</td>
<td>Bonjour Gateway forwarding policy</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configure a captive portal</td>
</tr>
<tr>
<td>clear</td>
<td>Clear</td>
</tr>
<tr>
<td>client-identity</td>
<td>Client identity (DHCP Device Fingerprinting)</td>
</tr>
<tr>
<td>client-identity-group</td>
<td>Client identity group (DHCP Fingerprint Database)</td>
</tr>
<tr>
<td>clone</td>
<td>Clone configuration object</td>
</tr>
<tr>
<td>customize</td>
<td>Customize the output of summary cli commands</td>
</tr>
<tr>
<td>device</td>
<td>Configuration on multiple devices</td>
</tr>
<tr>
<td>device-categorization</td>
<td>Configure a device categorization object</td>
</tr>
<tr>
<td>dhcp-server-policy</td>
<td>DHCP server policy</td>
</tr>
<tr>
<td>dns-whitelist</td>
<td>Configure a whitelist</td>
</tr>
<tr>
<td>event-system-policy</td>
<td>Configure a event system policy</td>
</tr>
<tr>
<td>firewall-policy</td>
<td>Configure firewall policy</td>
</tr>
<tr>
<td>global-association-list</td>
<td>Configure a global association list</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
</tr>
<tr>
<td>host</td>
<td>Enter the configuration context of a device by specifying its hostname</td>
</tr>
<tr>
<td>igmp-snoop-policy</td>
<td>Create igmp snoop policy</td>
</tr>
<tr>
<td>inline-password-encryption</td>
<td>Store encryption key in the startup configuration file</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>L2tpv3 tunnel protocol</td>
</tr>
<tr>
<td>mac</td>
<td>MAC configuration</td>
</tr>
<tr>
<td>management-policy</td>
<td>Configure a management policy</td>
</tr>
<tr>
<td>meshpoint</td>
<td>Create a new MESHPOINT or enter MESHPOINT configuration context for one or more MESHPOINTs</td>
</tr>
<tr>
<td>meshpoint-qos-policy</td>
<td>Configure a meshpoint quality-of-service policy</td>
</tr>
<tr>
<td>mint-policy</td>
<td>Configure the global mint policy</td>
</tr>
<tr>
<td>nac-list</td>
<td>Configure a network access control list</td>
</tr>
<tr>
<td>no</td>
<td></td>
</tr>
<tr>
<td>nx45xx</td>
<td>NX45XX integrated services platform</td>
</tr>
<tr>
<td>nx65xx</td>
<td>NX65XX integrated services platform</td>
</tr>
<tr>
<td>nx75xx</td>
<td>NX75XX wireless controller</td>
</tr>
<tr>
<td>passpoint-policy</td>
<td>Configure a passpoint policy</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Encrypt passwords in configuration</td>
</tr>
<tr>
<td>profile</td>
<td>Profile related commands - if no parameters are given, all profiles are selected</td>
</tr>
<tr>
<td>radio-qos-policy</td>
<td>Configure a radio quality-of-service policy</td>
</tr>
<tr>
<td>radius-group</td>
<td>Configure radius user group parameters</td>
</tr>
<tr>
<td>radius-server-policy</td>
<td>Create device onboard radius policy</td>
</tr>
<tr>
<td>radius-user-pool-policy</td>
<td>Configure Radius User Pool</td>
</tr>
<tr>
<td>rename</td>
<td>Clone configuration object</td>
</tr>
<tr>
<td>rf-domain</td>
<td>Create a RF Domain or enter rf-domain context</td>
</tr>
</tbody>
</table>
GLOBAL CONFIGURATION COMMANDS

for one or more rf-domains

rfs4000  RFS4000 wireless controller
rfs6000  RFS6000 wireless controller
rfs7000  RFS7000 wireless controller
role-policy  Role based firewall policy
routing-policy  Policy Based Routing Configuration
self  Config context of the device currently logged into

smart-cache-policy  Configure a content caching
smart-rf-policy  Configure a Smart-RF policy
wips-policy  Configure a wips policy
wlan  Create a new WLAN or enter WLAN configuration context for one or more WLANs
wlan-qos-policy  Configure a wlan quality-of-service policy
write  Write running configuration to memory or terminal

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
revert  Revert changes

service  Service Commands
show  Show running system information

<DEVICE>(config)#
4.1 Global Configuration Commands

Table 4.1 summarizes the Global Configuration 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 4-7</td>
</tr>
<tr>
<td>aaa-tacacs-policy</td>
<td>Configures AAA-TACACS policy</td>
<td>page 4-8</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, VLAN, and service aliases</td>
<td>page 4-9</td>
</tr>
<tr>
<td>ap300</td>
<td>Adds an AP300 to the network, and creates a general profile for the access point</td>
<td>page 4-17</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 4-27</td>
</tr>
<tr>
<td>ap6562</td>
<td>Adds an AP6562 to the network</td>
<td>page 4-28</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Adds an AP71XX to the network</td>
<td>page 4-29</td>
</tr>
<tr>
<td>ap7502</td>
<td>Adds an AP7502 to the network</td>
<td>page 4-24</td>
</tr>
<tr>
<td>ap7522</td>
<td>Adds an AP7522 to the network</td>
<td>page 4-25</td>
</tr>
<tr>
<td>ap7532</td>
<td>Adds an AP7532 to the network</td>
<td>page 4-26</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Adds an AP81XX to the network</td>
<td>page 4-30</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Adds an AP82XX to the network</td>
<td>page 4-31</td>
</tr>
<tr>
<td>association-acl-policy</td>
<td>Configures an association ACL policy</td>
<td>page 4-32</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 4-33</td>
</tr>
<tr>
<td>bonjour-gw-discovery-policy</td>
<td>Configures a Bonjour GW Discovery policy (RFS7000 and AP7131)</td>
<td>page 4-34</td>
</tr>
<tr>
<td>bonjour-gw-forwarding-policy</td>
<td>Configures a Bonjour GW Forwarding policy (RFS7000 and AP7131)</td>
<td>page 4-35</td>
</tr>
<tr>
<td>captive portal</td>
<td>Configures a captive portal</td>
<td>page 4-36</td>
</tr>
<tr>
<td>clear</td>
<td>Clears the event history</td>
<td>page 4-70</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>client-identity</td>
<td>Enables client identification through DHCP device fingerprinting</td>
<td>page 4-71</td>
</tr>
<tr>
<td>client-identity-group</td>
<td>Creates a new client identity group and enters its configuration mode</td>
<td>page 4-80</td>
</tr>
<tr>
<td>clone</td>
<td>Clones a specified configuration object</td>
<td>page 4-87</td>
</tr>
<tr>
<td>customize</td>
<td>Customizes the CLI command summary output</td>
<td>page 4-88</td>
</tr>
<tr>
<td>device</td>
<td>Specifies configuration on multiple devices</td>
<td>page 4-97</td>
</tr>
<tr>
<td>device-categorization</td>
<td>Configures a device categorization object</td>
<td>page 4-100</td>
</tr>
<tr>
<td>dhcp-server-policy</td>
<td>Configures a DHCP server policy</td>
<td>page 4-106</td>
</tr>
<tr>
<td>dns-whitelist</td>
<td>Configures a DNS whitelist</td>
<td>page 4-107</td>
</tr>
<tr>
<td>event-system-policy</td>
<td>Configures an event system policy</td>
<td>page 4-113</td>
</tr>
<tr>
<td>firewall-policy</td>
<td>Configures a firewall policy</td>
<td>page 4-127</td>
</tr>
<tr>
<td>global-association-list</td>
<td>Configures a global list of client MAC addresses</td>
<td>page 4-129</td>
</tr>
<tr>
<td>host</td>
<td>Sets the system’s network name</td>
<td>page 4-131</td>
</tr>
<tr>
<td>inline-password-encryption</td>
<td>Stores the encryption key in the startup configuration file</td>
<td>page 4-132</td>
</tr>
<tr>
<td>ip</td>
<td>Configures Internet Protocol (IP) components</td>
<td>page 4-133</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Configures Layer 2 Tunneling Protocol Version 3 (L2TPV3) tunnel policy</td>
<td>page 4-134</td>
</tr>
<tr>
<td>mac</td>
<td>Configures MAC access lists (goes to the MAC Access Control List (ACL) mode)</td>
<td>page 4-136</td>
</tr>
<tr>
<td>management-policy</td>
<td>Configures a management policy</td>
<td>page 4-137</td>
</tr>
<tr>
<td>meshpoint</td>
<td>Configures meshpoint related configuration commands</td>
<td>page 4-138</td>
</tr>
<tr>
<td>meshpoint-qos-policy</td>
<td>Configures a set of parameters that defines the quality of service (QoS)</td>
<td>page 4-139</td>
</tr>
<tr>
<td>mint-policy</td>
<td>Configures a MiNT security policy</td>
<td>page 4-140</td>
</tr>
<tr>
<td>nac-list</td>
<td>Configures a network ACL</td>
<td>page 4-141</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 4-147</td>
</tr>
<tr>
<td>passpoint-policy</td>
<td>Creates a new passpoint policy and enters its configuration mode</td>
<td>page 4-156</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Enables password encryption</td>
<td>page 4-158</td>
</tr>
<tr>
<td>profile</td>
<td>Configures profile related commands</td>
<td>page 4-159</td>
</tr>
<tr>
<td>radio-qos-policy</td>
<td>Configures a radio qos policy</td>
<td>page 4-166</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>radius-group</td>
<td>Configures a RADIUS group</td>
<td>page 4-167</td>
</tr>
<tr>
<td>radius-server-policy</td>
<td>Configures a RADIUS server policy</td>
<td>page 4-168</td>
</tr>
<tr>
<td>radius-user-pool-policy</td>
<td>Configures a RADIUS user pool policy</td>
<td>page 4-169</td>
</tr>
<tr>
<td>roaming-assist-policy</td>
<td>Configures a roaming assist policy</td>
<td>page 4-170</td>
</tr>
<tr>
<td>rename</td>
<td>Renames and existing top-level object (TLO)</td>
<td>page 4-171</td>
</tr>
<tr>
<td>rf-domain</td>
<td>Creates an RF Domain</td>
<td>page 4-175</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Adds an RFS4000 to the network</td>
<td>page 4-204</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Adds an RFS6000 to the network</td>
<td>page 4-205</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Adds an RFS7000 to the network</td>
<td>page 4-206</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Adds an NX45XX to the network</td>
<td>page 4-207</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Adds an NX65XX to the network</td>
<td>page 4-208</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Adds an NX75XX to the network</td>
<td>page 4-209</td>
</tr>
<tr>
<td>nx9000</td>
<td>Adds a NX9000, NX9500, or NX9510 to the network</td>
<td>page 4-210</td>
</tr>
<tr>
<td>role-policy</td>
<td>Configures a role policy</td>
<td>page 4-211</td>
</tr>
<tr>
<td>routing-policy</td>
<td>Configures a routing policy</td>
<td>page 4-212</td>
</tr>
<tr>
<td>self</td>
<td>Displays a logged device’s configuration context</td>
<td>page 4-213</td>
</tr>
<tr>
<td>smart-rf-policy</td>
<td>Configures a Smart RF policy</td>
<td>page 4-214</td>
</tr>
<tr>
<td>wips-policy</td>
<td>Configures a WIPS policy</td>
<td>page 4-215</td>
</tr>
<tr>
<td>wlan</td>
<td>Configures a wireless WLAN</td>
<td>page 4-217</td>
</tr>
<tr>
<td>wlan-qos-policy</td>
<td>Configures a WLAN QoS policy</td>
<td>page 4-284</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, NX9000, NX9500, and NX9510 series service platforms.</td>
<td>page 4-286</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 4-304</td>
</tr>
</tbody>
</table>
### 4.1.1 aaa-policy

**Global Configuration Commands**

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** — AP300, 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, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
aaa-policy <AAA-POLICY-NAME>
```

**Parameters**

- `aaa-policy <AAA-POLICY-NAME>`

| <AAA-POLICY-NAME> | Specify the AAA policy name. If the policy does not exist, it is created. |

**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

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

**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 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 — AP300, 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, NX9000, NX9500, NX9600, NX9510

**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 26, **AAA-TACACS-POLICY.**
4.1.3 alias

4.1.3.1 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.

- **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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9600, NX9510

**Syntax**

```
alias [address-range|bonjour-service|host|network|network-group|network-service|string|vlan]

alias bonjour-service <BONJOUR-SERVICE-ALIAS-NAME> <SERVICE-STRING>

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|ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www}


alias string <STRING-ALIAS-NAME> <LINE>

alias vlan <VLAN-ALIAS-NAME> <1-4094>
```
### Parameters

- **alias bonjour-service <BONJOUR-SERVICE-ALIAS-NAME> <SERVICE-STRING>**
  - **bonjour-service <BONJOUR-SERVICE-ALIAS-NAME>** Creates a Bonjour service alias, which maps a user-friendly to a service
    - **<BONJOUR-SERVICE-ALIAS-NAME>** – Specify the alias name. Use a user-friendly name that enables you to easily identify the associated Bonjour service.
    - For example, _home-sharing._tcp.local can be mapped to $homeshare.
    - **Note:** Alias name should begin with `$`.
  - **<SERVICE-STRING>** Specify the RFC name of the Bonjour service.
    - **Note:** This bonjour-service alias can be used in a bonjour-gw-discovery-policy. For more information, see `bonjour-gw-discovery-policy`.

- **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
    - **<ADDRESS-RANGE-ALIAS-NAME>** – Specify the address range alias name.
    - **Note:** Alias name should begin with `$`.
  - **<STARTING-IP> to <ENDING-IP>** Associates a range of IP addresses with this address range alias
    - **<STARTING-IP>** – Specify the first IP address in the range.
    - **to <ENDING-IP>** – Specify the last IP address in the range.

- **alias host <HOST-ALIAS-NAME> <HOST-IP>**
  - **host <HOST-ALIAS-NAME>** Creates a host alias, defining a single network host
    - **<HOST-ALIAS-NAME>** – Specify the host alias name.
    - **Note:** Alias name should begin with `$`.
  - **<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>**
  - **network <NETWORK-ALIAS-NAME>** Creates a network alias, defining a single network address
    - **<NETWORK-ALIAS-NAME>** – Specify the network alias name.
    - **Note:** Alias name should begin with `$`.
  - **<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.
### network `<NETWORK-GROUP-ALIAS-NAME>`

- **Creates a network-group alias**
- **<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.

### 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.

### host `<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>`

- **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|ntp|ntpt|pop3|proto|sip|smtp|sourceport (<1-65535>|<WORD>|ssh|telnet|tftp|www)}`

- **Configures an alias that specifies available 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:** 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.
### Global Configuration Commands

**GLOBAL CONFIGURATION COMMANDS**

**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* (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 48.
  - 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| nntp|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)
  - 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 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 $DOMAIN test.company.com`. In this example, the string alias name is: `$DOMAIN` and the string value it is mapped to is: `test.company.com`. In this example, the string alias refers to a domain name.

**Note:** Alias name should begin with `$`.

**Examples**

```
rfs4000-229D58(config)#alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
rfs4000-229D58(config)#
```

```
rfs4000-229D58(config)#alias network $TestNetworkAlias 192.168.13.0/24
rfs4000-229D58(config)#
```

```
rfs4000-229D58(config)#alias host $TestHostAlias 192.168.13.10
rfs4000-229D58(config)#
```

```
rfs4000-229D58(config)#alias vlan $TestVLANAlias 1
rfs4000-229D58(config)#
```

```
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
```

```
! Configuration of RFS4000 version 5.5.6.0-006D
!
! 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 vlan $TestVLANAlias 1

ip access-list BROADCAST-MULTICAST-CONTROL
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
--More--
rfs4000-229D58(config)#

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

```
rfs4000-229D58(config)#alias string $DOMAIN test.company.com
```

```
rfs4000-229D58(config)#show context
```

```
! Configuration of RFS4000 version 5.5.6.0-006D
!
version 2.3
!
---More---

Related Commands

| no | Removes an existing network, VLAN, service, or string alias |
4.1.4 ap300

Global Configuration Commands

Adds an AP300 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

NOTE: This command is not supported on the NX45XX, NX75XX, NX9XXX and NX65XX series service platforms.

Syntax

```
pap {<MAC>}
```

Parameters

- `ap300 {<MAC>}`

  `<MAC>` Optional. Specify the AP300's MAC address.
  When this command is issued without any parameters, the default AP300 profile is configured.

Examples

```
rfs7000-37FABE(config)#ap300 00-A0-F8-CF-1E-DA

rfs7000-37FABE(config-ap300-00-A0-F8-CF-1E-DA)#
```

```
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CP1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

```
rfs7000-37FABE(config)#
```

Related Commands

- `no` Removes an AP300 from the network
### 4.1.5 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap621 <MAC>
```

**Parameters**
- `ap621 <MAC>`

<table>
<thead>
<tr>
<th>&lt;MAC&gt;</th>
<th>Specify the AP621's MAC address.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs7000-37FABE(config)#ap621 5C-0E-8B-E3-C3-56
rfs7000-37FABE(config-device-5C-0E-8B-E3-C3-56)#
```

```
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>
</tbody>
</table>
+-------------+-----------------+-----------+-----------+-----------+---------------------+
```

```
rfs7000-37FABE(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>no</th>
<th>Removes an AP621 from the network</th>
</tr>
</thead>
</table>

4.1.6 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap622 <MAC>
```

**Parameters**

- ap622 <MAC>

| <MAC> | Specify the AP622's MAC address. |

**Examples**

```
rfs7000-37FABE(config)#ap622 B4-C7-99-43-C3-DC
rfs7000-37FABE(config-device-B4-C7-99-43-C3-DC)#
```

```
rfs7000-37FABE(config)#show wireless ap configured
---------------------------------------------------------------------------------------
IDX         NAME                MAC              PROFILE       RF-DOMAIN    ADOPTED-BY
---------------------------------------------------------------------------------------
1    ap7131-889EC4      00-15-70-88-9E-C4   default-ap7131    default     un-adopted
2    ap300-CF1EDA       00-A0-F8-CF-1E-DA   default-ap300     default     un-adopted
3    ap621-E3C356       5C-0E-8B-E3-C3-56   default-ap621     default     un-adopted
4    ap622-43C3DC       B4-C7-99-43-C3-DC   default-ap622     default     un-adopted
---------------------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

**Related Commands**

```
no
```

Removes an AP622 from the network
4.1.7 **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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap650 <MAC>
```

**Parameters**

- `ap650 <MAC>`

| <MAC> | Specify the AP650's MAC address. |

**Examples**

```
rfs7000-37FABE(config)#ap650 5C-0E-8B-34-81-BC
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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** | Removes an AP650 from the network |

---

**Supported in the following platforms:**

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

**Syntax**

```
ap650 <MAC>
```

**Parameters**

- `ap650 <MAC>`

| <MAC> | Specify the AP650's MAC address. |

**Examples**

```
rfs7000-37FABE(config)#ap650 5C-0E-8B-34-81-BC
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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** | Removes an AP650 from the network |

---
4.1.8 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
```
ap6511 <MAC>
```

Parameters
- `ap6511 <MAC>`

| <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)#
```
```
rfs7000-37FABE(config)#show wireless ap configured
---------------------------------------------------------------------------------------
IDX   NAME                MAC              PROFILE       RF-DOMAIN    ADOPTED-BY
---------------------------------------------------------------------------------------
 1    ap7131-889EC4      00-15-70-88-9E-C4   default-ap7131    default     un-adopted
 2    ap300-CF1EDA       00-A0-F8-CF-1E-DA   default-ap300     default     un-adopted
 3    ap621-E3C356       5C-0E-8B-E3-C3-56   default-ap621     default     un-adopted
 4    ap622-43C3DC       B4-C7-99-43-C3-DC   default-ap622     default     un-adopted
 5    ap650-3481BC       5C-0E-8B-34-81-BC   default-ap650     default     un-adopted
 6    ap6511-08456A      5C-0E-8B-08-45-6A   default-ap6511    default     un-adopted
---------------------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

Related Commands
```
no
Removes an AP6511 from the network
```

4.1.9 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ap6521 <MAC>`

**Parameters**

- `<MAC>`

  Specify the AP6521’s MAC address.

**Examples**

```
rfs7000-37FABE(config)#ap6521 5C-0E-8B-08-73-68
rfs7000-37FABE(config-device-5C-0E-8B-08-73-68)#
```

```
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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>6</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>7</td>
<td>ap6521-087368</td>
<td>5C-0E-8B-08-73-68</td>
<td>default-ap6521</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>
```

```
rfs7000-37FABE(config)#
```

**Related Commands**

- `no` Removes an AP6521 from the network
4.1.10 *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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap6522 <MAC>
```

**Parameters**

- `<MAC>` Specify the AP6522's MAC address.

**Examples**

```
rfs7000-37FABE(config)#ap6522 5C-0E-8B-7B-F2-24
rfs7000-37FABE(config-device-5C-0E-8B-7B-F2-24)#
```

```
rfs7000-37FABE(config)#show wireless ap configured
---------------------------------------------------------------------
IDX | NAME                | MAC              | PROFILE       | RF-DOMAIN | ADOPTED-BY   
---------------------------------------------------------------------
 1  | ap7131-889EC4       | 00-15-70-88-9E-C4| default-ap7131| default   | un-adopted   
 2  | ap300-CF1EDA        | 00-A0-F8-CF-1E-DA| default-ap300 | default   | un-adopted   
 3  | ap621-E3C356        | 5C-0E-8B-E3-C3-56| default-ap621 | default   | un-adopted   
 4  | ap622-43C3DC        | B4-C7-99-43-C3-DC| default-ap622 | default   | un-adopted   
 5  | ap650-3481BC        | 5C-0E-8B-34-81-BC| default-ap650 | default   | un-adopted   
 6  | ap6511-08456A       | 5C-0E-8B-08-45-6A| default-ap6511| default   | un-adopted   
 7  | ap6521-087368       | 5C-0E-8B-08-73-68| default-ap6521| default   | un-adopted   
 8  | ap6522-7BF224       | 5C-0E-8B-7B-F2-24| default-ap6522| default   | un-adopted   
---------------------------------------------------------------------
rfs7000-37FABE(config)#
```

**Related Commands**

```
no
```

Removes an AP6522 from the network
4.1.11 ap7502

Global Configuration Commands

Adds an AP7502 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

ap7502 <MAC>

Parameters

- ap7502 <MAC>

| <MAC> | Specify the AP7502's MAC address. |

Examples

rfs7000-37FABE(config)#ap7502 00-23-09-E-12-66

Related Commands

- no Removes an AP7502 from the network
4.1.12 *ap7522*

*Global Configuration Commands*

Adds an AP7522 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, NX6500, NX6524, NX7500, 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
```

**Related Commands**

- *no* Removes an AP7522 from the network
4.1.13 *ap7532*

*Global Configuration Commands*

Adds an AP7532 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
ap7532 <MAC>
```

**Parameters**

- `ap7532 <MAC>`

<table>
<thead>
<tr>
<th>&lt;MAC&gt;</th>
<th>Specify the AP7532's MAC address.</th>
</tr>
</thead>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config)#ap7532 00-23-09-0E-12-71
```

**Related Commands**

- `no` Removes an AP7532 from the network
4.1.14 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap6532 <MAC>
```

**Parameters**

- `ap6532 <MAC>`

**Examples**

```
rfs7000-37FABE(config)#ap6532 00-23-68-31-16-59
rfs7000-37FABE(config-device-00-23-68-31-16-59)#
```

```
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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>6</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>7</td>
<td>ap6521-087368</td>
<td>5C-0E-8B-08-73-68</td>
<td>default-ap6521</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>8</td>
<td>ap6522-7BF224</td>
<td>5C-0E-8B-7B-F2-24</td>
<td>default-ap6522</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>9</td>
<td>ap6532-311659</td>
<td>00-23-68-31-16-59</td>
<td>default-ap6532</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

```
rfs7000-37FABE(config)#
```

**Related Commands**

```
no
```

Removes an AP6532 from the network
4.1.15 **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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ap6562 <MAC>
```

**Parameters**
- **ap6562** `<MAC>`

---

**Examples**

```
rfs7000-37FABE(config)#ap6532 00-23-09-0E-12-60
rfs7000-37FABE(config-device-00-23-09-0E-12-60)#
```

```
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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>6</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>7</td>
<td>ap6521-087368</td>
<td>5C-0E-8B-08-73-68</td>
<td>default-ap6521</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>8</td>
<td>ap6522-7BF224</td>
<td>5C-0E-8B-7B-F2-24</td>
<td>default-ap6522</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>9</td>
<td>ap6532-311659</td>
<td>00-23-68-31-16-59</td>
<td>default-ap6532</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>10</td>
<td>ap6562-0E1260</td>
<td>00-23-09-0E-12-60</td>
<td>default-ap6562</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

```
rfs7000-37FABE(config)#
```

**Related Commands**

- **no** Removes an AP6562 from the network
4.1.16 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

ap71xx <MAC>

Parameters

- ap71xx <MAC>

Examples

rfs7000-37FABE(config)#ap71xx 00-23-68-99-BF-A8
rfs7000-37FABE(config-device-00-23-68-99-BF-A8)#

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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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>6</td>
<td>ap6511-08456A</td>
<td>5C-0E-8B-08-45-6A</td>
<td>default-ap651</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>7</td>
<td>ap6521-087368</td>
<td>5C-0E-8B-08-73-68</td>
<td>default-ap6521</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>8</td>
<td>ap6522-7BF224</td>
<td>5C-0E-8B-7B-F2-24</td>
<td>default-ap6522</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>9</td>
<td>ap6532-311659</td>
<td>00-23-68-31-16-59</td>
<td>default-ap653</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>10</td>
<td>ap6562-0E1260</td>
<td>00-23-09-0E-12-60</td>
<td>default-ap6562</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>11</td>
<td>ap7131-99BFA8</td>
<td>00-23-68-99-BF-A8</td>
<td>default-ap71xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

Related Commands

no

Removes an AP71XX 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
ap81xx <MAC>

Parameters
- ap81xx <MAC>

Examples
rfs7000-37FABE(config)#ap81xx C4-01-FA-BE-F1-16
rfs7000-37FABE(config-device-C4-01-FA-BE-F1-16)#

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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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>6</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>7</td>
<td>ap6521-087368</td>
<td>5C-0E-8B-08-73-68</td>
<td>default-ap6521</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>8</td>
<td>ap6522-7BF224</td>
<td>5C-0E-8B-7B-F2-24</td>
<td>default-ap6522</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>9</td>
<td>ap6532-311659</td>
<td>00-23-68-31-16-59</td>
<td>default-ap6532</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>10</td>
<td>ap6562-OB1260</td>
<td>00-23-09-0E-12-60</td>
<td>default-ap6562</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>11</td>
<td>ap7131-99BFA8</td>
<td>00-23-68-99-BF-A8</td>
<td>default-ap71xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>12</td>
<td>ap8132-BEF116</td>
<td>C4-01-FA-BE-F1-16</td>
<td>default-ap81xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
</tbody>
</table>

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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ap82xx <MAC>`

**Parameters**

- `ap82xx` `<MAC>`

**Examples**

```
  rfs7000-37FABE(config)#ap82xx 6C-90-CD-02-54-21
  rfs7000-37FABE(config-device-6C-90-CD-02-54-21)#
```

```
rfs7000-37FABE(config)#show wireless ap configured
---------------------------------------------------------------------------------------
IDX         NAME                MAC              PROFILE       RF-DOMAIN    ADOPTED-BY
---------------------------------------------------------------------------------------
 1    ap7131-889EC4      00-15-70-88-9E-C4   default-ap7131    default     un-adopted
 2    ap300-CF1EDA       00-A0-F8-CF-1E-DA   default-ap300     default     un-adopted
 3    ap621-E3C356       5C-0E-8B-E3-C3-56   default-ap621     default     un-adopted
 4    ap622-43C3DC       B4-C7-99-43-C3-DC   default-ap622     default     un-adopted
 5    ap650-3481BC       5C-0E-8B-34-81-BC   default-ap650     default     un-adopted
 6    ap6511-08456A      5C-0E-8B-08-45-6A   default-ap6511    default     un-adopted
 7    ap6521-087368      5C-0E-8B-08-73-68   default-ap6521    default     un-adopted
 8    ap6522-7BF224      5C-0E-8B-7B-F2-24   default-ap6522    default     un-adopted
 9    ap6532-311659      00-23-68-31-16-59   default-ap6532    default     un-adopted
 10   ap6562-0E1260      00-23-09-0E-12-60   default-ap6562    default     un-adopted
 11   ap7131-99BFA8      00-23-68-99-BF-A8   default-ap71xx    default     un-adopted
 12   ap8132-BEF116      C4-01-FA-BE-F1-16   default-ap81xx    default     un-adopted
 13   ap8232-147748      00-23-68-14-77-48   default-ap82xx    default     un-adopted
---------------------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

**Related Commands**

- `no` Removes an AP82XX from the network
4.19 association-acl-policy

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 — AP300, 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, 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
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-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.
4.1.20 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP811X, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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          Assign default profile and default rf-domain
  deny            Add rule to deny device adoption
  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
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-auto-provisioning-policy-test)#

Related Commands

no

NOTE: For more information on the association-acl-policy, see Chapter 9, AUTO-PROVISIONING-POLICY.
4.1.21 **bonjour-gw-discovery-policy**

**Global Configuration Commands**

Configures a Bonjour GW Discovery policy. The policy defines a list of services clients want to discover across subnets. When configured and applied, this feature enables Bonjour services on local and tunneled VLANs.

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS7000

**Syntax**

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

**Parameters**

- `bonjour-gw-discovery-policy <POLICY-NAME>`

**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
  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 Bonjour GW Discovery policy
4.1.22 **bonjour-gw-forwarding-policy**

- **Global Configuration Commands**

  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.

  To receive Bonjour service responses from specific VLANs, specify the VLAN IDs. You can provide a list of VLAN IDs in the following format: 10-20, 25, 30-35.

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS7000

**Syntax**

`bonjour-gw-forwarding-policy <POLICY-NAME>`

**Parameters**

- `bonjour-gw-forwarding-policy <POLICY-NAME>`

<table>
<thead>
<tr>
<th><code>&lt;POLICY-NAME&gt;</code></th>
<th>Specify the Bonjour GW Forwarding policy name. If the policy does not exist, it is created.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>To receive Bonjour service responses from specific VLANs, specify the VLAN IDs. In the Bonjour GW Forwarding policy configuration mode, provide a list of VLAN IDs from which Bonjour responses can be received (format: 10-20, 25, 30-35). And then specify the list of client VLANs that can access Bonjour services.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Execute the <code>bonjour-gw-discovery-policy</code> command to define the Bonjour services allowed on local and tunneled VLANs.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To associate a Bonjour GW Forwarding policy with a device or profile, in the profile/device configuration mode, execute the <code>use &gt; bonjour-gw-forwarding-policy &gt; &lt;POLICY-NAME&gt;</code> command. For more information see, <code>use</code>.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
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

```plaintext
rfs7000-37FABE(config-bonjour-gw-forwarding-policy-TestPolicy)#
```

**Related Commands**

- `no` Removes an existing Bonjour GW Forwarding policy
4.1.23 captive portal

- Global Configuration Commands

A captive portal provides secure guest access and authentication services within the network. Table 4.2 lists the command to enter the captive portal configuration mode.

Table 4.2 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 4-37</td>
</tr>
<tr>
<td>captive-portal-mode</td>
<td>Summarizes captive portal configuration commands</td>
<td>page 4-39</td>
</tr>
</tbody>
</table>
4.1.23.1 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 — AP300, 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, NX7500, 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
- `logout-fqdn` Configure the FQDN address to logout the session from client
- `no` Negate a command or set its defaults
- `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

Specify the captive portal name. If the captive portal does not exist, it is created.
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.
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

| no | Removes an existing captive portal |
### 4.1.23 captive-portal-mode commands

Table 4.3 summarizes captive portal configuration mode commands.

**Table 4.3** Captive-Portal-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 4-40</td>
</tr>
<tr>
<td>access-type</td>
<td>Configures a captive portal’s access type</td>
<td>page 4-41</td>
</tr>
<tr>
<td>accounting</td>
<td>Enables a captive portal’s accounting records</td>
<td>page 4-42</td>
</tr>
<tr>
<td>bypass</td>
<td>Enables bypassing of captive portal detection requests</td>
<td>page 4-44</td>
</tr>
<tr>
<td>connection-mode</td>
<td>Configures a captive portal’s connection mode</td>
<td>page 4-45</td>
</tr>
<tr>
<td>custom-auth</td>
<td>Configures custom user information</td>
<td>page 4-46</td>
</tr>
<tr>
<td>data-limit</td>
<td>Enforces data limit on captive portal clients</td>
<td>page 4-47</td>
</tr>
<tr>
<td>inactivity-timeout</td>
<td>Defines an inactivity timeout in seconds</td>
<td>page 4-48</td>
</tr>
<tr>
<td>logout-fqdn</td>
<td>Clears the logout FQDN address</td>
<td>page 4-49</td>
</tr>
<tr>
<td>no</td>
<td>Reverts the selected captive portal’s settings to default</td>
<td>page 4-50</td>
</tr>
<tr>
<td>post-authentication-vlan</td>
<td>Assigns a post authentication RADIUS VLAN for this captive portal’s users</td>
<td>page 4-55</td>
</tr>
<tr>
<td>radius-vlan-assignment</td>
<td>Assigns a RADIUS VLAN for this captive portal</td>
<td>page 4-56</td>
</tr>
<tr>
<td>redirection</td>
<td>Enables redirection of client connections to specified destination ports</td>
<td>page 4-57</td>
</tr>
<tr>
<td>server</td>
<td>Configures the captive portal server settings</td>
<td>page 4-58</td>
</tr>
<tr>
<td>simultaneous-users</td>
<td>Specifies a username used by a MAC address pool</td>
<td>page 4-60</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 4-61</td>
</tr>
<tr>
<td>use</td>
<td>Associates a AAA policy and a DNS whitelist with a captive portal</td>
<td>page 4-62</td>
</tr>
<tr>
<td>webpage</td>
<td>Configures captive portal Web page settings</td>
<td>page 4-63</td>
</tr>
<tr>
<td>webpage-auto-upload</td>
<td>Enables automatic upload of advanced Web pages on a captive portal</td>
<td>page 4-68</td>
</tr>
<tr>
<td>webpage-location</td>
<td>Specifies the location of Web pages used for captive portal authentication</td>
<td>page 4-69</td>
</tr>
</tbody>
</table>
4.1.23.2.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

access-time <10-10080>

Parameters

- access-time <10-10080>

| <10-10080> | Defines the access time allowed for a wireless client from 10 - 10080 minutes. The default is 1440 minutes. |

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)
**4.1.23.2.2 access-type**

*captivate-portal-mode commands*

Defines the captive portal's access type

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`access-type [custom-auth-radius|email|logging|no-auth|radius]`

**Parameters**

- `access-type [custom-auth-radius|email|logging|no-auth|radius]`

<table>
<thead>
<tr>
<th>custom-auth-radius</th>
<th>Specifies the custom user information used for authentication (RADIUS lookup of given information, such as name, e-mail address, telephone etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>When selecting this option, use the custom-auth command to configure the required user information.</td>
</tr>
<tr>
<td>email</td>
<td>Uses user's e-mail address for authentication</td>
</tr>
<tr>
<td>logging</td>
<td>Logs records of users and allowed access. The system logs user access details.</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>
</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
```

**Related Commands**

- `no` | Removes the captive portal access type or reverts to default (radius)
4.1.23.2.3 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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. 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)#
| no       | Disables accounting records for this captive portal |
4.1.23.2.4 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 — AP300, 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, 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 bypass captive-portal-detection

rfs4000-229D58(config-captive-portal-test)#

**Related Commands**

| no | Disables bypassing of captive portal detection requests |
4.1.23.2.5 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, it is recommended to HTTPS, as it affords controller and client transmissions some measure of data protection HTTP cannot provide.

Supported in the following platforms:
- Access Points — AP300, 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, 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>

Note: HTTPS is a more secure version of HTTP, and uses encryption while sending and receiving requests.

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
4.1.23.2.6 custom-auth

- **captive-portal-mode commands**

Configures custom user information

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

custom-auth info <LINE>

**Parameters**

- **custom-auth info <LINE>**

<table>
<thead>
<tr>
<th>info &lt;LINE&gt;</th>
<th>Configures information used for RADIUS lookup when custom-auth RADIUS access type is configured</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;LINE&gt; – Guest data needs to be provided. Specify the name, e-mail address, and telephone number of the user.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-captive-portal-test)#custom-auth info bob, bob@company.com

rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
  access-type logging
  access-time 35
  custom-auth info bob, bob@company.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
4.1.23.2.7 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 — AP300, 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, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-limit</td>
<td>Sets a captive portal client's data transfer limit in megabytes. This limit is applicable for both upstream and downstream data transfer.</td>
</tr>
<tr>
<td>action</td>
<td>Optional. Specifies the action taken when a client exceeds the configured data limit. The options are:</td>
</tr>
<tr>
<td></td>
<td>log-and-disconnect – Logs a record and disconnects the client</td>
</tr>
<tr>
<td></td>
<td>log-only – Only a log is generated and the client remains connected to the captive portal. This is the default setting.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-captive-portal-test)#data-limit 200 action log-and-disconnect
rfs7000-37FABE(config-captive-portal-test)#

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
4.1.23.2.8 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

 Syntax

 inactivity-timeout <300-86400>

 Parameters

 - inactivity-timeout <300-86400>

<table>
<thead>
<tr>
<th>&lt;300-86400&gt;</th>
<th>Defines the timeout interval after which a captive portal session is automatically terminated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;300-86400&gt; – Specify a value from 300 - 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@company.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
4.1.23.2.9 logout-fqdn

**captive-portal-mode commands**

Configures the *Fully Qualified Domain Name* (FQDN) address to logout of the session from the client.

Supported in the following platforms:
- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
logout-fqdn <WORD>
```

**Parameters**
- **logout-fqdn <WORD>**

<table>
<thead>
<tr>
<th>logout-fqdn &lt;WORD&gt;</th>
<th>Configures the FQDN address used to logout</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>– Provide the FQDN address (for example, logout.guestaccess.com).</td>
</tr>
</tbody>
</table>

**Examples**
```
rfs7000-37FABE(config-captive-portal-test)#logout-fqdn logout.testuser.com
rfs7000-37FABE(config-captive-portal-test)#
```
```
rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
  logout-fqdn logout.testuser.com
rfs7000-37FABE(config-captive-portal-test)#
```

**Related Commands**
```
no
```
Clears the logout FQDN address.
4.1.23.2.10 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [access-time|access-type|accounting|bypass|connection-mode|custom-auth|data-limit|inactivity-timeout|logout-fqdn|post-authentication-vlan|radius-vlan-assignment|redirection|server|simultaneous-users|terms-agreement|use|webpage|webpage-auto-upload|webpage-location]

no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|logout-fqdn|post-authentication-vlan|radius-vlan-assignment|simultaneous-users|terms-agreement|use|webpage-auto-upload|webpage-location]

no accounting [radius|syslog]

no bypass captive-portal-detection

no custom-auth info

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|welcome]

no webpage internal [org-name|org-signature]

no webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]

no webpage internal [description|footer|header|main-logo|small-logo|title]
```

**Parameters**

- no [access-time|access-type|connection-mode|data-limit|inactivity-timeout|logout-fqdn|post-authentication-vlan|radius-vlan-assignment|simultaneous-users|terms-agreement|use|webpage|webpage-auto-upload|webpage-location]

<table>
<thead>
<tr>
<th>no access-time</th>
<th>Resets client access time</th>
</tr>
</thead>
<tbody>
<tr>
<td>no access-type</td>
<td>Resets client access type</td>
</tr>
<tr>
<td>no connection-mode</td>
<td>Resets connection mode to HTTP</td>
</tr>
<tr>
<td>no data-limit</td>
<td>Removes data limit enforcement for captive portal clients</td>
</tr>
<tr>
<td>no inactivity-timeout</td>
<td>Resets inactivity timeout interval</td>
</tr>
<tr>
<td>no logout-fqdn</td>
<td>Clears the logout FQDN address</td>
</tr>
<tr>
<td>no post-authentication-vlan</td>
<td>Removes the post authentication RADIUS VLAN assigned to this captive portal’s users</td>
</tr>
<tr>
<td>no radius-vlan-assignment</td>
<td>Disables RADIUS VLAN assignment for captive portal users</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>no simultaneous-users</td>
<td>Resets the number of MAC addresses that can use a single user name to its default of 1</td>
</tr>
<tr>
<td>no terms-agreement</td>
<td>Resets the terms of agreement required for logging in. The user no longer has to agree to terms &amp; conditions before connecting to a captive portal.</td>
</tr>
<tr>
<td>no webpage-auto-upload</td>
<td>Disables automatic upload of advanced Web pages on a captive portal.</td>
</tr>
<tr>
<td>no webpage-location</td>
<td>Resets the use of custom Web pages for login, welcome, terms, and failure page. The default is automatically created Web pages.</td>
</tr>
<tr>
<td>no accounting [radius</td>
<td>syslog]</td>
</tr>
<tr>
<td>radius</td>
<td>Disables support for sending RADIUS accounting messages</td>
</tr>
<tr>
<td>syslog</td>
<td>Disables support for sending syslog messages to remote syslog servers</td>
</tr>
<tr>
<td>no bypass captive-portal-detection</td>
<td>Disables bypassing of captive-portal detection requests</td>
</tr>
<tr>
<td>no custom-auth info</td>
<td>Resets custom authentication information</td>
</tr>
<tr>
<td>info</td>
<td>Resets the configuration of custom user information sent to the RADIUS server (for custom-auth-radius access type)</td>
</tr>
<tr>
<td>no redirection ports</td>
<td>Disables redirection of client connections to specified destination ports</td>
</tr>
<tr>
<td>no server host</td>
<td>Clears captive portal server address</td>
</tr>
<tr>
<td>no server mode [centralized-controller [hosting-vlan-interface]]</td>
<td>Clears the captive portal server mode</td>
</tr>
<tr>
<td>centralized-controller</td>
<td>Optional. Resets the hosting VLAN interface for centralized captive portal server to its default of zero (0)</td>
</tr>
<tr>
<td>hosting-vlan-interface</td>
<td></td>
</tr>
<tr>
<td>no use [aaa-policy</td>
<td>dns-whitelist]</td>
</tr>
<tr>
<td>aaa-policy</td>
<td>Removes the AAA policy used with a captive portal policy</td>
</tr>
<tr>
<td>dns-whitelist</td>
<td>Removes the DNS whitelist used with a captive portal policy</td>
</tr>
</tbody>
</table>
- **no webpage external** [acknowledgment|agreement|fail|login *post*|no-service|welcome]

  **no webpage external** Resets the external Web pages settings. These are the Web pages (externally located) displayed when a user interacts with the captive portal.

  **acknowledgment** Resets the acknowledgment page settings

  **agreement** Resets the agreement page settings

  **fail** Resets the fail page settings

  **login *post*** Resets the login page settings

  - *post* – Optional. Users are redirected to post internally when they try to authenticate

  **no-service** Resets the no-service page settings. The no-service Web page is displayed when critical services (such as, AAA server, captive portal server, DHCP server, and AP to controller connectivity) are not reachable and the user cannot access the captive portal.

  **welcome** Resets the welcome page settings

- **no webpage internal** [org-name|org-signature]

  **no webpage internal** Resets the configuration of internal Web pages displayed when a user interacts with the captive portal

  **org-name** Resets the organization name that is included at the top of Web pages

  **org-signature** Resets the organization signature (email, addresses, phone numbers) included at the bottom of Web pages

- **no webpage internal** [acknowledgment|agreement|fail|login|no-service|welcome] [description|footer|header|main-logo|small-logo|title]

  **no webpage internal** Resets the internal Web pages settings. These are the Webpages (internally located) displayed when a user interacts with the captive portal.

  **acknowledgment** Resets the acknowledgment page settings

  **agreement** Resets the agreement page settings

  **fail** Resets the fail page settings

  **login** Resets the login page settings

  **no-service** Resets the no-service page settings. The no-service Web page is displayed when critical services (such as, AAA server, captive portal server, DHCP server) are not reachable and the user cannot access the captive portal.

  **welcome** Resets the welcome page settings

  **description** Resets the description part of each Web page. This is the area where information about the captive portal and user state is displayed to the user.

  **footer** Resets the footer portion of each Web page. A footer can contain the organization signature.

  **header** Resets the header portion of each Web page

  **main-logo** Resets the main logo of each Web page
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@company.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@company.com
  connection-mode https
  inactivity-timeout 750
rfs7000-37FABE(config-captive-portal-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-time</td>
<td>Configures the allowed access time for each captive portal client</td>
</tr>
<tr>
<td>access-type</td>
<td>Configures captive portal authentication and logging information</td>
</tr>
<tr>
<td>accounting</td>
<td>Configures captive portal accounting information</td>
</tr>
<tr>
<td>bypass</td>
<td>Enables bypassing of captive portal detection requests</td>
</tr>
<tr>
<td>connection-mode</td>
<td>Configures how clients connect to a captive portal</td>
</tr>
<tr>
<td>custom-auth</td>
<td>Configures the captive portal parameters required for client access</td>
</tr>
<tr>
<td>inactivity-timeout</td>
<td>Configures the client inactivity timeout interval</td>
</tr>
<tr>
<td>logout-fqdn</td>
<td>Configures the FQDN address to logout of the session from the client</td>
</tr>
<tr>
<td>post-authentication-vlan</td>
<td>Assigns a post authentication RADIUS VLAN for this captive portal’s users</td>
</tr>
<tr>
<td>radius-vlan-assignment</td>
<td>Enables assignment of a RADIUS VLAN for this captive portal</td>
</tr>
<tr>
<td>redirection</td>
<td>Enables redirection of client connections to specified destination ports</td>
</tr>
<tr>
<td>server</td>
<td>Configures captive portal server parameters</td>
</tr>
<tr>
<td>simultaneous-users</td>
<td>Configures the maximum number of clients that can use a single captive portal user name</td>
</tr>
<tr>
<td>terms-agreement</td>
<td>Configures if a client has to accept terms and conditions before logging to the captive portal</td>
</tr>
<tr>
<td>use</td>
<td>Associates a AAA policy and DNS whitelist with this captive portal policy</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>webpage-location</td>
<td>Configures the location of Web pages displayed when the user interacts with the captive portal</td>
</tr>
<tr>
<td>webpage</td>
<td>Configures Web pages used by the captive portal to interact with users</td>
</tr>
<tr>
<td>webpage-auto-upload</td>
<td>Enables automatic upload of advanced Web pages on a captive portal</td>
</tr>
<tr>
<td>aaa-policy</td>
<td>Configures a AAA policy</td>
</tr>
<tr>
<td>dns-whitelist</td>
<td>Configures a DNS whitelist</td>
</tr>
</tbody>
</table>
### 4.1.23.2.11 post-authentication-vlan

**captive-portal-mode commands**

Assigns a post authentication RADIUS VLAN for this captive portal’s users.

**Supported in the following platforms:**
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

`post-authentication-vlan <1-4096>`

**Parameters**

- `post-authentication-vlan <1-4096>`

<table>
<thead>
<tr>
<th>post-authentication-vlan &lt;1-4096&gt;</th>
<th>Assigns a VLAN for this captive portal’s users after they have authenticated and logged on to the network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;1-4096&gt;</code> – Specify the VLAN’s number from 1 - 4096.</td>
</tr>
</tbody>
</table>

**Examples**

```
ras4000-229D58(config-captive-portal-test)#post-authentication-vlan 1
ras4000-229D58(config-captive-portal-test)#

ras4000-229D58(config-captive-portal-test)#show context captive-portal test post-authentication-vlan 1
ras4000-229D58(config-captive-portal-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>no</th>
<th>Removes the post authentication RADIUS VLAN assigned to this captive portal’s users</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-vlan-assignment</td>
<td>Enables assignment of a RADIUS VLAN for this captive portal</td>
</tr>
</tbody>
</table>
4.1.23.2.12 radius-vlan-assignment

► captive-portal-mode commands

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 — AP300, 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, 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)#

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>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>
4.1.23.2.13 redirection

- **captive-portal-mode commands**

Enables redirection of client connections to specified destination ports

Supported in the following platforms:

- Access Points — AP300, 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, 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>
</table>

**Examples**

rfs4000-229D58(config-captive-portal-test)#redirection ports 1,2,3
rfs4000-229D58(config-captive-portal-test)#

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
4.1.23.2.14 server

* captive-portal-mode commands

Configures captive portal server parameters, such as the hostname, IP, and mode of operation

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
server [host|mode]
server host <IP/HOSTNAME>
server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]

Parameters
- server host <IP/HOSTNAME>

  host <IP/HOSTNAME> Configures the internal captive portal authentication server (wireless controller, access point, service platform)
  - <IP/HOSTNAME> – Specify the IP address or hostname of the captive portal server.
  
  Note: For centralized wireless controller mode, this should be a virtual hostname and not IP address.

- server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]

  mode Configures the captive portal server mode
  - centralized
    - 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.
  
  centralized-controller {hosting-vlan-interface <0-4096>}
  - 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.
    - 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.
    - <0-4096> – Specify the VLAN number (0 implies the controller is available on the client’s VLAN).
  
  self
  - 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.

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@company.com
custom-mode https
inactivity-timeout 750
server host 172.16.10.9
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 host and mode settings</td>
</tr>
</tbody>
</table>
4.1.23.2.15 simultaneous-users

**captive-portal-mode commands**

Specifies the number of MAC addresses that can simultaneously use a particular username. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

simultaneous-users <1-8192>

**Parameters**

- simultaneous-users <1-8192>

| <1-8192> | Specifies the number of MAC addresses that can simultaneously use a particular username. Select a number from 1 - 8192. |

**Examples**

```bash
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@company.com
  connection-mode https
  inactivity-timeout 750
  server host 172.16.10.9
  simultaneous-users 5

rfs7000-37FABE(config-captive-portal-test)#ab
```

**Related Commands**

- **no** Resets or disables captive portal commands
4.1.23.2.16 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.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, 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@company.com
connection-mode https
inactivity-timeout 750
server host 172.16.10.9
simultaneous-users 5
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 commands</td>
</tr>
</tbody>
</table>
4.1.23.2.17 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]
```

**Parameters**

- `use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-policy</td>
<td>Configures a AAA policy with this captive portal. AAA policies validate user credentials and provide captive portal access to the network.</td>
</tr>
<tr>
<td>&lt;AAA-POLICY-NAME&gt;</td>
<td>Specify the AAA policy name.</td>
</tr>
<tr>
<td>dns-whitelist</td>
<td>Configures a DNS whitelist to use with this captive portal. DNS whitelists restrict captive portal access.</td>
</tr>
<tr>
<td>&lt;DNS-WHITELIST-NAME&gt;</td>
<td>Specify the DNS whitelist name.</td>
</tr>
</tbody>
</table>

**Note:** To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be added to the DNS whitelist.

**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@company.com
  connection-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><code>no</code></td>
<td>Removes a DNS Whitelist or a AAA policy from the captive portal</td>
</tr>
<tr>
<td><code>dns-whitelist</code></td>
<td>Configures a DNS whitelist</td>
</tr>
<tr>
<td><code>aaa-policy</code></td>
<td>Configures a AAA policy</td>
</tr>
</tbody>
</table>
4.1.23.2.18 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. There are six (6) different pages.

- 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 unavailability of critical services.
- 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
webpage [external|internal]
webpage external [acknowledgment|agreement|fail|login {post}|no-service|welcome] <URL>
webpage internal [acknowledgment|agreement|fail|login|no-service|org-name|org-signature|welcome]
    [description|footer|header|title] <CONTENT>
webpage internal [acknowledgment|agreement|fail|login|no-service|welcome]
    [main-logo|small-logo] <URL>
webpage internal [org-name|org-signature] <LINE>
```

Parameters

- webpage external [acknowledgment|agreement|fail|login {post}|no-service|welcome] <URL>
  - external
    Indicates Web pages being served are hosted on an external (to the captive portal) server resource.
  - acknowledgment
    Indicates the page is displayed for user acknowledgment of details. Users are redirected to this page to acknowledge information provided.
  - agreement
    Indicates the page is displayed for “Terms & Conditions”.
    The agreement page provides conditions that must be agreed to before captive portal access is permitted.
<table>
<thead>
<tr>
<th>fail</th>
<th>Indicates the page is displayed for login failure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>login {post}</th>
<th>Indicates the page is displayed for getting user credentials. This page is displayed by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• post – Optional. Redirects users to post externally when they during authentication</td>
</tr>
<tr>
<td></td>
<td>The login page prompts the user for a username and password to access the captive portal and proceed to either the agreement page (if used) or the welcome page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no-service</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated</td>
</tr>
<tr>
<td></td>
<td>• The external captive portal server is not reachable</td>
</tr>
<tr>
<td></td>
<td>• The connectivity between the adopted AP and controller is lost</td>
</tr>
<tr>
<td></td>
<td>• The external DHCP server is not reachable</td>
</tr>
<tr>
<td></td>
<td>To provide this service, enable the following:</td>
</tr>
<tr>
<td></td>
<td>• External captive portal server monitoring</td>
</tr>
<tr>
<td></td>
<td>• AAA server monitoring. This enables detection of RADIUS server failure.</td>
</tr>
<tr>
<td></td>
<td>• External DHCP server monitoring</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For more information on enabling these critical resource monitoring, see service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>welcome</th>
<th>Indicates the page is displayed after a user has been successfully authenticated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The welcome page asserts a user has logged in successfully and can access the captive portal.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;URL&gt;</th>
<th>Indicates the URL to the Web page displayed. Query String: URL can include query tags. Supported Query Tags are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 'WING_TAG_CLIENT_IP' - Captive portal client IPv4 address</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_CLIENT_MAC' - Captive portal client MAC address</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_WLAN_SSID' - Captive portal client WLAN ssid</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_AP_MAC' - Captive portal client AP MAC address</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_AP_NAME' - Captive portal client AP Name</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_CP_SERVER' - Captive portal server address</td>
</tr>
<tr>
<td></td>
<td>• 'WING_TAG_USERNAME' - Captive portal authentication username</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><a href="http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&amp;ap_m">http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&amp;ap_m</a></td>
</tr>
<tr>
<td></td>
<td>c=WING_TAG_AP_MAC. Use ‘&amp;’ or ‘?’ character to separate field-value pair. Note: Enter ‘ctrl-v’ followed by ‘?’ to configure query string</td>
</tr>
</tbody>
</table>
**webpage internal** [acknowledgment|agreement|fail|login|no-service|welcome] [description|footer|header|title] <CONTENT>

<table>
<thead>
<tr>
<th>internal</th>
<th>Indicates the Web pages are internal. 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 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></td>
<td>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated</td>
</tr>
<tr>
<td></td>
<td>• The external captive portal server is not reachable</td>
</tr>
<tr>
<td></td>
<td>• The connectivity between the adopted AP and controller is lost</td>
</tr>
<tr>
<td></td>
<td>• The external DHCP server is not reachable</td>
</tr>
<tr>
<td></td>
<td>To provide this service, enable the following:</td>
</tr>
<tr>
<td></td>
<td>• External captive portal server monitoring</td>
</tr>
<tr>
<td></td>
<td>• AAA server monitoring. This enables detection of RADIUS server failure.</td>
</tr>
<tr>
<td></td>
<td>• External DHCP server monitoring</td>
</tr>
<tr>
<td></td>
<td>• AP to controller connectivity monitoring</td>
</tr>
<tr>
<td>welcome</td>
<td>Indicates the page is displayed after a user has been successfully authenticated</td>
</tr>
<tr>
<td>description</td>
<td>Indicates the content is the description portion of each of the following internal Web pages:</td>
</tr>
<tr>
<td></td>
<td>acknowledgment, agreement, fail, login, no-service, and welcome</td>
</tr>
<tr>
<td>footer</td>
<td>Indicates the content is the footer portion of each of the following internal Web pages:</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>acknowledgment, agreement, fail, no-service, and welcome page. The title for each of these pages is configured here.</td>
</tr>
<tr>
<td>&lt;CONTENT&gt;</td>
<td>The following keyword is common to all of the above internal Web page options:</td>
</tr>
<tr>
<td></td>
<td>• &lt;CONTENT&gt; – 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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>internal</td>
<td>Indicates the Web pages are internal</td>
</tr>
<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                                  |
| welcome      | Indicates the page is displayed after a user has been successfully authenticated |
| main-logo    | The following keyword is common to all of the above internal Web page options:  
|              | • main-logo – Indicates the main logo displayed in the header portion of each Web page |
| small-logo   | The following keyword is common to all of the above internal Web page options:  
|              | • small-logo – Indicates the logo image displayed in the footer portion of each Web page, and constitutes the organization’s signature |
| <URL>        | Provides the complete URL of the main-logo and small-logo files             |
|              | • <URL> – Specify the location of the main-logo and the small-logo files. The files are loaded from the specified location. |
| org-name     | Specifies the company’s name, included on Web pages along with the main image |
| org-signature | Specifies the company’s signature information, included in the bottom of Web pages along with a small image |
| <LINE>       | Specify the company’s name or signature depending on the option selected.    |
Examples

rfs7000-37FABE(config-captive-portal-test)#webpage external fail http://www.company.com

rfs7000-37FABE(config-captive-portal-test)#show context captive-portal test
  access-time 35
  custom-auth info bob,\ bob@company.com
  connection-mode https
  inactivity-timeout 750
  server host 172.16.10.9
  simultaneous-users 5
  terms-agreement
  webpage-location external
  webpage external fail http://www.company.com
  use aaa-policy test
rfs7000-37FABE(config-captive-portal-test)#

Related Commands

| no | Resets or disables captive portal configurations |
4.1.23.2.19 webpage-auto-upload

Enables automatic upload of advanced Web pages on a captive portal. 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 — AP300, 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, 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)#

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>
4.1.23.2.20 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 — AP300, 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, 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 advanced 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 webpage-auto-upload option to automatically launch the advanced pages to requesting clients upon association. For more information, see webpage-auto-upload.</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@company.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>no</td>
<td>Resets or disables captive portal Web page settings</td>
</tr>
<tr>
<td>webpage</td>
<td>Configures a captive portal's Web page (acknowledgment, agreement, login, welcome, fail, no-service, and terms) settings</td>
</tr>
<tr>
<td>webpage-auto-upload</td>
<td>Enables an automatic upload of advanced Web pages on a captive portal</td>
</tr>
</tbody>
</table>
4.1.24 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** — AP300, 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, 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 '2014-01-31 00:15:57 UTC' by 'admin'

2014-01-31 00:15:36     rfs4000-229D58  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-01-30 23:43:10     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.224' authentication successful
2014-01-30 03:47:47     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
'admin' with privilege 'superuser' from '192.168.100.231(web)'
2014-01-30 02:45:08     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.231' authentication successful
2014-01-28 20:28:29     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
'admin' with privilege 'superuser' from '192.168.100.173(web)'
2014-01-28 19:56:31     rfs4000-229D58  SYSTEM     UI_USER_AUTH_SUCCESS UI user
'admin' from: '192.168.100.173' authentication successful
2014-01-27 20:15:20     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
'admin' with privilege 'superuser' from '192.168.100.204'
2014-01-27 20:14:45     rfs4000-229D58  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
'admin' with privilege 'superuser' from '192.168.100.204'
logged in user 'admin' with privilege 'superuser' from 'ssh'

--More--
rfs4000-229D58#
```

```
rfs4000-229D58#clear event-history
rfs4000-229D58#
```

```
rfs4000-229D58#show event-history
EVENT HISTORY REPORT
Generated on '2014-02-15 14:59:21 UTC' by 'admin'

rfs4000-229D58#
```
### 4.1.25 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.

Table 4.4 summarizes the commands available for creating and configuring a set of new client identity parameters.

**Table 4.4 Client-Identity-Config Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>client-identity</code></td>
<td>Creates a new client identity and enters its configuration mode</td>
<td>page 4-72</td>
</tr>
<tr>
<td><code>client-identity-mode commands</code></td>
<td>Invokes the client identity policy configuration mode commands</td>
<td>page 4-74</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 4-80</td>
</tr>
</tbody>
</table>
4.1.25.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
client-identity <CLIENT-IDENTITY-NAME>

Parameters
- client-identity <CLIENT-IDENTITY-NAME>

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)#?

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)#
4.1.25.2 client-identity-mode commands

- client-identity

Table 4.5 summarizes a new client’s identity configuration mode commands.

**Table 4.5 Client-Identity-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 4-75</td>
</tr>
<tr>
<td>dhcp-match-message-type</td>
<td>Configures the DHCP message type for device fingerprinting</td>
<td>page 4-78</td>
</tr>
<tr>
<td>no</td>
<td>Removes the DHCP option (used for client identification) configurations</td>
<td>page 4-79</td>
</tr>
</tbody>
</table>
### 4.1.25.2.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

dhcp <1-16> [message-type|option|option-modes]

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>
</tbody>
</table>

**Note:** A maximum of 16 match criteria can be configured.

<table>
<thead>
<tr>
<th>message-type</th>
<th>Specifies the message type to which this DHCP match criteria is applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>discover</td>
<td>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.</td>
</tr>
<tr>
<td>request</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note:** It is recommended to configure client-identity with request messages, because clients rarely send discover messages.

**Note:** If the message type is not specified, the fingerprint is checked with all message types (DHCP request and DHCP discover).

<table>
<thead>
<tr>
<th>option &lt;1-254&gt;</th>
<th>The following keywords are common to the ‘discover’ and ‘request’ message types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>option</td>
<td>Configures a DHCP option value, which is used as the match criteria</td>
</tr>
<tr>
<td>&lt;1-254&gt;</td>
<td>Configures a code for this DHCP option from 1 - 254 (except option 53)</td>
</tr>
</tbody>
</table>
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, it is recommended to use the combination of one or more of the preceding options to define a device.

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes a DHCP option signature (match criteria)</td>
</tr>
</tbody>
</table>
4.1.25.2.2 dhcp-match-message-type

Configures the DHCP message type to match

Supported in the following platforms:
- Access Points — AP300, 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, 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)#

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
4.1.25.2.3 no

▶ client-identity-mode commands

Removes the DHCP options match criteria configurations

Supported in the following platforms:

• Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [dhcp|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  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-16&gt; – Specify the DHCP option match criteria rule index</td>
</tr>
</tbody>
</table>

| 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

<table>
<thead>
<tr>
<th>dhcp</th>
<th>Configures the DHCP option match criteria for device fingerprinting</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-match-message-type</td>
<td>Configures the DHCP message type for device fingerprinting</td>
</tr>
</tbody>
</table>
4.1.26 client-identity-group

Table 4.6 summarizes the commands for creating and configuring a new client identity group.

<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 4-81</td>
</tr>
<tr>
<td>client-identity-group-mode</td>
<td>Invokes the client identity group configuration mode commands</td>
<td>page 4-82</td>
</tr>
<tr>
<td>client-identity</td>
<td>Creates new client identity policy and enters its configuration mode</td>
<td>page 4-71</td>
</tr>
</tbody>
</table>
4.1.26.1 client-identity-group

- **client-identity-group**

Configures 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

client-identity-group <CLIENT-IDENTITY-GROUP-NAME> precedence <1-10000>

**Parameters**

- **client-identity-group <CLIENT-IDENTITY-GROUP-NAME> <1-10000>**

<table>
<thead>
<tr>
<th>client-identity-group &lt;CLIENT-IDENTITY-GROUP-NAME&gt;</th>
<th>Creates a new client identity group and enters its configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>precedence &lt;1-10000&gt;</td>
<td>Specifies a precedence value for this client identity match criteria in this client identity group</td>
</tr>
</tbody>
</table>

**Note:** Client identity signatures with lower precedence are evaluated first.

**Examples**

rfs4000-229D58(config)#client-identity-group test
rfs4000-229D58(config-client-identity-group-test)#

rfs4000-229D58(config-client-identity-group-test)#?  
Client Identity group Mode commands:
- client-identity Client identity (DHCP Device Fingerprinting)  
- 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-group-test)#
4.1.26.2 client-identity-group-mode commands

Table 4.5 summarizes a new client identity group configuration mode commands.

**Table 4.7 Client-Identity-Group-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 fingerprinting) with this client identity group</td>
<td>page 4-83</td>
</tr>
<tr>
<td>no</td>
<td>Removes the client identity associated with this client identity group</td>
<td>page 4-79</td>
</tr>
</tbody>
</table>
4.26.2.1 client-identity

**client-identity-group-mode commands**

Associates an existing and configured client identity (device fingerprinting) with this client identity group

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5000, NX5024, NX6500, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

**Parameters**

- **client-identity** `<CLIENT-IDENTITY-NAME>` precedence `<1-10000>`

<table>
<thead>
<tr>
<th><strong>client-identity</strong> <code>&lt;CLIENT-IDENTITY-NAME&gt;</code></th>
<th>Associates a client identity with this group</th>
</tr>
</thead>
<tbody>
<tr>
<td>precedence <code>&lt;1-10000&gt;</code></td>
<td>Determines the order in which client identity is used.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
rfs4000-229D58(config)# show context
!
! Configuration of RFS4000 version 5.5.6.0-006D
!
! 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"
permit udp any eq 67 any eq dhcp rule-precedence 11 rule-description "permit D
--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 5.5.6.0-006D
!
! 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"
!
! client-identity Android-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-4
  dhcp 8 message-type request option 55 exact hexstring 012103061c333a3b
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-4-1-X
  dhcp 1 message-type request option 55 exact hexstring 012103060f1c333a3b
  dhcp 2 message-type request option 60 exact ascii dhcpcd-5.2.10
!
! client-identity Android-4-2-X
  dhcp 1 message-type request option 55 exact hexstring 012103060f1c333a3b
  dhcp 2 message-type request option 60 exact ascii dhcpcd-5.5.6
!
! client-identity Galaxy-Note
  dhcp 8 message-type request option 55 exact hexstring 012103061c333a3b
dhcp 9 message-type request option 60 exact ascii dhcpcd-5.2.10:Linux-3.0.15-N7000DDLP8-CL551076:armv7l:SMDK4210
!
! client-identity Galaxy-Tab
  dhcp 8 message-type request option 55 exact hexstring 012103061c333a3b
dhcp 9 message-type request option 60 exact ascii dhcpcd-5.2.10:Linux-2.6.36.3:armv7l:p3
Related Commands

```
n0 | Removes the client identity associated with the client identity group
```
4.1.26.2.2 no

**client-identity-group-mode commands**

Removes the client identity associated with the client identity group

Supported in the following platforms:
- Access Points — AP300, 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, 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>— Specify the client identity name.</td>
</tr>
</tbody>
</table>

**Examples**

rfs4000-229D58(config-client-identity-group-test)# show context
client-identity-group test
client-identity test precedence 1
rfs4000-229D58(config-client-identity-group-test)#

rfs4000-229D58(config-client-identity-group-test)# no client-identity test
rfs4000-229D58(config)#

**Related Commands**

- **client-identity** Associates an existing and configured client identity (device fingerprinting) with this client identity group
4.1.27 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 modify only the required parameters.

Supported in the following platforms:

- Access Points — AP300, 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, 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>
  
  TLO <EXISTING-OBJECT-NAME>  
  <NEW-OBJECT-NAME>
  
  Creates a new TLO by cloning an existing top-level object. The new object has the same configuration as the cloned object.
  
  - <EXISTING-OBJECT-NAME> — Specify the existing object’s (to be cloned) name
  - <NEW-OBJECT-NAME> — Provide the new object’s name.
  
  Note: Enter clone and press Tab to list objects available for cloning.

- clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>

  device  
  <EXISTING-DEVICE-MAC/NAME>  
  <NEW-DEVICE-MAC>

  Configures a new device based on an existing device configuration
  
  - <EXISTING-DEVICE-MAC/NAME> — Specify the existing device’s name or MAC address (the device to be cloned)
  - <NEW-DEVICE-MAC> — Provide the new device’s MAC address.
  
  Note: Enter clone > device and press Tab to list devices available for cloning.

Examples

rfs7000-37FABE(config)#clone rf_domain RF_Domain_Cloned RF_Domain_New
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show context

! Configuration of RFS7000 version 5.5.6.0-006D
!

version 2.1

customize show-wireless-client mac ip vendor vlan radio-id state wlan location radio-
alias radio-type

.................................................................
!

rf-domain RF_Domain_New
location Bangalore
contact tpg483@company.com
timezone Asia/Calcutta
country-code in
--More--
rfs7000-37FABE(config)#
4.1.28 customize

Global Configuration Commands

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax


customize hostname-column-width <1-64>

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, 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, t-index, tx-rate)

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, 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-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, 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)

Parameters
- customize hostname-column-width <1-64>

<table>
<thead>
<tr>
<th>hostname-column-width &lt;1-64&gt;</th>
<th>Configures default width of the hostname column in all show commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</td>
<td></td>
</tr>
</tbody>
</table>
- **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)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show-wireless-client</td>
<td>Customizes the show wireless client command output</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></td>
<td>• &lt;1-64&gt; – Sets the ap-name column width from 1 - 64 characters</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></td>
<td>• &lt;1-32&gt; – Sets the client-identity column width from 1 - 32 characters</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, tx-bytes, tx-dropped, tx-packets, tx-throughput)**

<table>
<thead>
<tr>
<th>show-wireless-client-stats</th>
<th>Customizes the show wireless client stats command output</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>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>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, noise, q-index, rx-rate, signal, snr, t-index, tx-rate)**

<table>
<thead>
<tr>
<th>show-wireless-client-stats-rf</th>
<th>Customizes the show wireless client stats RF command output</th>
</tr>
</thead>
<tbody>
<tr>
<td>average-retry-number</td>
<td>Includes the average-retry-number column, which displays the average number of retransmissions made per packet</td>
</tr>
<tr>
<td>error-rate</td>
<td>Includes the error-rate column, which displays the rate of error for 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>mac</td>
<td>Includes the MAC column, which displays the wireless client’s MAC address</td>
</tr>
<tr>
<td>noise</td>
<td>Includes the noise column, which displays the noise (in dBm) as detected by the wireless client</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><strong>Note</strong>: Higher values indicate better RF quality.</td>
</tr>
<tr>
<td>rx-rate</td>
<td>Includes the rx-rate column, which displays the receive rate at the particular wireless client</td>
</tr>
<tr>
<td>signal</td>
<td>Includes the signal column, which displays the signal strength (in dBm) at the particular wireless client</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snr</td>
<td>Includes the snr column, which displays the signal to noise (SNR) ratio (in dB) at the particular 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-rate</td>
<td>Includes the tx-rate column, which displays the packet transmission rate at the particular wireless client</td>
</tr>
</tbody>
</table>

- 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)

<table>
<thead>
<tr>
<th>show-wireless-meshpoint</th>
<th>Customizes the show wireless meshpoint command output</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>
<tr>
<td>hostname &lt;1-64&gt;</td>
<td>Includes the hostname column, which displays the AP's hostname. Applicable only in case of non-wireless controller meshpoints</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</td>
</tr>
<tr>
<td>interface-ids</td>
<td>Includes the interface-ids column, which displays the interface identifiers (interfaces used by this meshpoint)</td>
</tr>
<tr>
<td>is-root</td>
<td>Includes the is-root column, which displays the current root state of the meshpoint</td>
</tr>
<tr>
<td>mesh-name &lt;1-64&gt;</td>
<td>Includes the mesh-name column, which displays the meshpoint's name</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Sets the mesh-name column width from 1 - 64 characters</td>
</tr>
<tr>
<td>mpid</td>
<td>Includes the mpid column, which displays the meshpoint identifier in the AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>next-hop-hostname &lt;1-64&gt;</td>
<td>Includes the next-hop-hostname column, which displays the next-hop AP's name (the AP next in the path to the bound root)</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-64&gt; – Sets the next-hop-hostname column width from 1 - 64 characters</td>
</tr>
<tr>
<td>next-hop-ifid</td>
<td>Includes the next-hop-ifid column, which displays the next-hop interface identifier in the AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>next-hop-use-time</td>
<td>Includes the next-hop-use-time column, which displays the time since this meshpoint started using this next hop</td>
</tr>
<tr>
<td>root-bound-time</td>
<td>Includes the root-bound-time column, which displays the time since this meshpoint has been bound to the current root</td>
</tr>
<tr>
<td>Customize</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>customize show-wireless-meshpoint-neighbor-stats</code></td>
<td>Customizes the show wireless meshpoint neighbor stats command output</td>
</tr>
</tbody>
</table>
| `ap-name <1-64>` | Includes the ap-name column, which displays name of the AP reporting a neighbor  
   • `<1-64>` – Sets the ap-name column width from 1 - 64 characters |
| `neighbor-hostname <1-64>` | Includes the neighbor-hostname column, which displays the reported neighbor’s hostname  
   • `<1-64>` – Sets the neighbor-hostname column width from 1 - 64 characters |
| `neighbor-ifid` | Includes the neighbor-ifid column, which displays the neighbor’s interface ID |
| `rx-bytes` | Includes the rx-bytes column, which displays the total bytes received |
| `rx-errors` | Includes the rx-error column, which displays the total bytes of error received |
| `rx-packets` | Includes the rx-packets column, which displays the number of packets received |
| `rx-throughput` | Includes the rx-throughput column, which displays neighbor’s received throughput |
| `tx-bytes` | Includes the tx-bytes column, which displays the total bytes transmitted |
| `tx-dropped` | Includes the tx-dropped column, which displays the total bytes dropped |
| `tx-packets` | Includes the tx-packets column, which displays the number of packets transmitted |
| `tx-throughput` | Includes the tx-throughput column, which displays neighbor’s transmitted throughput |

<table>
<thead>
<tr>
<th>Customize</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>customize show-wireless-meshpoint-neighbor-stats-rf</code></td>
<td>Customizes the show wireless meshpoint neighbor statistics RF command output</td>
</tr>
</tbody>
</table>
| `ap-name <1-64>` | Includes the ap-name column, which displays name of the AP reporting a neighbor  
   • `<1-64>` – Sets the ap-name column width from 1 - 64 characters |
| `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 |
| `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 |
<table>
<thead>
<tr>
<th>noise</th>
<th>Includes the noise column, which displays the noise level in dBm</th>
</tr>
</thead>
<tbody>
<tr>
<td>q-index</td>
<td>Includes the q-index column, which displays the q-index</td>
</tr>
<tr>
<td>rx-rate</td>
<td>Includes the rx-rate column, which displays rate of receiving</td>
</tr>
<tr>
<td>signal</td>
<td>Includes the signal column, which displays the signal strength in dBm</td>
</tr>
<tr>
<td>snr</td>
<td>Includes the snr column, which displays the signal-to-noise ratio</td>
</tr>
<tr>
<td>t-index</td>
<td>Includes the t-index column, which displays t-index</td>
</tr>
<tr>
<td>tx-rate</td>
<td>Includes the tx-rate column, which displays rate of transmission</td>
</tr>
</tbody>
</table>

- 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>show-wireless-radio</th>
<th>Customizes the show wireless radio command output</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopt-to</td>
<td>Includes the adopt-to column, which displays information about the wireless controller adopting this AP</td>
</tr>
<tr>
<td>ap-name &lt;1-64&gt;</td>
<td>Includes the ap-name column, which displays information about the AP this radio belongs</td>
</tr>
<tr>
<td>channel</td>
<td>Includes the channel column, which displays information about the configured and current channel for this radio</td>
</tr>
<tr>
<td>location &lt;1-64&gt;</td>
<td>Includes the location column, which displays the location of the AP this radio belongs</td>
</tr>
<tr>
<td>num-clients</td>
<td>Includes the num-clients column, which displays the number of clients associated with this radio</td>
</tr>
<tr>
<td>power</td>
<td>Includes the power column, which displays the radio’s configured and current transmit power</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 &quot;HOSTNAME:RX&quot; format)</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>rf-mode</td>
<td>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.</td>
</tr>
<tr>
<td>state</td>
<td>Includes the state column, which displays the radio’s current operational state</td>
</tr>
</tbody>
</table>

- 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)

<p>| show-wireless-radio-stats | Customizes the show wireless radio statistics command output |</p>
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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-bytes</td>
<td>Includes the rx-bytes column, which displays the total number of bytes received by the radio</td>
</tr>
<tr>
<td>rx-errors</td>
<td>Includes the rx-error column, which displays the total number of errors received by the radio</td>
</tr>
<tr>
<td>rx-packets</td>
<td>Includes the rx-packets column, which displays the total number of packets received by the radio</td>
</tr>
<tr>
<td>rx-throughput</td>
<td>Includes the rx-throughput column, which displays the receive throughput at the radio</td>
</tr>
<tr>
<td>tx-bytes</td>
<td>Includes the tx-bytes column, which displays the total number of bytes transmitted by the radio</td>
</tr>
<tr>
<td>tx-dropped</td>
<td>Includes the tx-dropped column, which displays the total number of packets dropped by the radio</td>
</tr>
<tr>
<td>tx-packets</td>
<td>Includes the tx-packets column, which displays the total number of packets transmitted by the radio</td>
</tr>
<tr>
<td>tx-throughput</td>
<td>Includes the tx-throughput column, which displays the transmission throughput at the radio</td>
</tr>
<tr>
<td></td>
<td>• customize show-wireless-radio-stats-rf (average-retry-number, error-rate, noise, q-index, radio-alias &lt;3-67&gt;, radio-id, radio-mac, rx-rate, signal, snr, t-index, tx-rate)</td>
</tr>
<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>
</tbody>
</table>
Examples

rfs7000-37FABE(config)#customize show-wireless-client ap-name auth
rfs7000-37FABE(config)#commit
rfs7000-37FABE(config)#show wireless client

<table>
<thead>
<tr>
<th>AP-NAME</th>
<th>AUTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------</td>
<td>------</td>
</tr>
</tbody>
</table>

Total number of wireless clients displayed: 0
rfs7000-37FABE(config)#

The following examples demonstrate how to customize the `show > wireless > meshpoint` command output.

The following example shows the `show > wireless > meshpoint` command output format before customization:

```
rfs4000-1B3596#show wireless meshpoint
```

```
<table>
<thead>
<tr>
<th>MESH</th>
<th>HOSTNAME</th>
<th>IS-ROOT</th>
<th>CONFIG-AS-ROOT</th>
<th>ROOT-BOUND-TIME</th>
<th>NEXT-HOP-HOSTNAME</th>
<th>NEXT-HOP-USE-TIME</th>
<th>INTERFACE-IDENTIFIERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>c00466</td>
<td>ap7131-96F998</td>
<td>1</td>
<td>NO</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:10:04</td>
<td>ap7131-96FAAC</td>
<td>00-23-68-93-16-60(00-23-68-96-F9-98:R1), 00-23-68-93-48-E1(00-23-68-96-F9-98:R2)</td>
</tr>
<tr>
<td>days 02:01:33</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:01:33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c00466</td>
<td>ap7131-96FAAC</td>
<td>0</td>
<td>YES</td>
<td>YES</td>
<td>N/A</td>
<td>N/A</td>
<td>00-23-68-95-23-51(00-23-68-96-FA-AC:R2)</td>
</tr>
<tr>
<td>c00466</td>
<td>ap7131-96F6B4</td>
<td>2</td>
<td>NO</td>
<td>NO</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:01:31</td>
<td>ap7131-96F998</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 3
rfs4000-1B3596#
```

The `show > wireless > meshpoint` command output is customized as follows:

```
rfs4000-1B3596(config)#customize show-wireless-meshpoint hops hostname 13 is-root config-as-root root-bound-time next-hop-hostname next-hop-use-time interface-ids
rfs4000-1B3596(config)#commit
```

The following example shows the `show > wireless > meshpoint` command output format after customization:

```
rfs4000-1B3596(config)#show wireless meshpoint
```

```
<table>
<thead>
<tr>
<th>HOPS</th>
<th>HOSTNAME</th>
<th>IS-ROOT</th>
<th>CONFIG-AS-ROOT</th>
<th>ROOT-BOUND-TIME</th>
<th>NEXT-HOP-HOSTNAME</th>
<th>NEXT-HOP-USE-TIME</th>
<th>INTERFACE-IDENTIFIERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ap7131-96F998</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>N/A</td>
<td>N/A</td>
<td>N/</td>
<td></td>
</tr>
<tr>
<td>00-23-68-93-16-60(00-23-68-96-F9-98:R1), 00-23-68-93-48-E1(00-23-68-96-F9-98:R2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00-23-68-95-23-51(00-23-68-96-FA-AC:R2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 ap7131-96F6B4</td>
<td>NO</td>
<td>1 days 02:10:08</td>
<td>ap7131-96F998</td>
<td>1 days 02:10:08</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:10:04</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:10:08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00-23-68-95-33-31(00-23-68-96-F6-B4:R2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 3
rfs4000-1B3596(config)#

`t-index` Includes the `t-index` column, which displays the traffic utilization index at the particular radio

`tx-rate` Includes the `tx-rate` column, which displays the packet transmission rate at the particular radio
To revert to the default format use the `no > customize` command.

```
rfs4000-1B3596(config)#no customize show-wireless-meshpoint
rfs4000-1B3596(config)#commit
```

The `show > wireless > meshpoint` command output format has been reverted to default.

```
rfs4000-1B3596(config)#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</td>
<td>NO</td>
<td>NO</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:10:40</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:10:40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c00466</td>
<td>ap7131-96FAAC</td>
<td>0</td>
<td>YES</td>
<td>YES</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c00466</td>
<td>ap7131-96F6B4</td>
<td>2</td>
<td>NO</td>
<td>NO</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:10:38</td>
<td>ap7131-96FAAC</td>
<td>1 days 02:10:38</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 3

rfs4000-1B3596(config)#

**Related Commands**

- **no**
  - Restores custom CLI settings to default

- **wireless**
  - Displays wireless configuration and other information
4.1.29 device

Global Configuration Commands

Enables simultaneous configuration of multiple devices

Supported in the following platforms:

- Access Points — AP300, 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, 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|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|
nx65xx|nx75xx|nx9000]}

device filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]}

Parameters

- device containing <STRING> {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|
ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|
nx65xx|nx75xx|nx9000]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td>Configures a basic device profile</td>
</tr>
<tr>
<td>containing &lt;STRING&gt;</td>
<td>Configures the string to search for in the device's hostname. Only those devices that have the specified string in their hostname can be configured.</td>
</tr>
<tr>
<td>filter type</td>
<td>Optional. Filters out a specific device type</td>
</tr>
<tr>
<td>ap621</td>
<td>Optional. Filters out all devices other than AP621s</td>
</tr>
<tr>
<td>ap622</td>
<td>Optional. Filters out all devices other than AP622s</td>
</tr>
<tr>
<td>ap650</td>
<td>Optional. Filters out devices other than AP650s</td>
</tr>
<tr>
<td>ap6511</td>
<td>Optional. Filters out devices other than AP6511s</td>
</tr>
<tr>
<td>ap6521</td>
<td>Optional. Filters out devices other than AP6521s</td>
</tr>
<tr>
<td>ap6522</td>
<td>Optional. Filters out devices other than AP6522s</td>
</tr>
<tr>
<td>ap6532</td>
<td>Optional. Filters out devices other than AP6532s</td>
</tr>
<tr>
<td>ap6562</td>
<td>Optional. Filters out devices other than AP6562s</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Optional. Filters out devices other than AP71XXs</td>
</tr>
<tr>
<td>ap7502</td>
<td>Filters out devices other than AP7502</td>
</tr>
<tr>
<td>ap7522</td>
<td>Filters out devices other than AP7522</td>
</tr>
<tr>
<td>ap7532</td>
<td>Filters out devices other than AP7532</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Optional. Filters out devices other than AP81XXs</td>
</tr>
<tr>
<td>device</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Optional. Filters out devices other than AP82XXs</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Optional. Filters out devices other than RFS4000s</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Optional. Filters out devices other than RFS6000s</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Optional. Filters out devices other than RFS7000s</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Optional. Filters out devices other than NX45XX series</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Optional. Filters out devices other than NX65XX series</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Optional. Filters out devices other than NX75XX series</td>
</tr>
<tr>
<td>nx9000</td>
<td>Optional. Filters out devices other than NX9000 series</td>
</tr>
<tr>
<td>ap621</td>
<td>Filters out all devices other than AP621s</td>
</tr>
<tr>
<td>ap622</td>
<td>Filters out all devices other than AP622s</td>
</tr>
<tr>
<td>ap650</td>
<td>Filters out devices other than AP650s</td>
</tr>
<tr>
<td>ap6511</td>
<td>Filters out devices other than AP6511s</td>
</tr>
<tr>
<td>ap6521</td>
<td>Filters out devices other than AP6521s</td>
</tr>
<tr>
<td>ap6522</td>
<td>Filters out devices other than AP6522s</td>
</tr>
<tr>
<td>ap6532</td>
<td>Filters out devices other than AP6532s</td>
</tr>
<tr>
<td>ap6562</td>
<td>Filters out devices other than AP6562s</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Filters out devices other than AP71XXs</td>
</tr>
<tr>
<td>ap7502</td>
<td>Filters out devices other than AP7502</td>
</tr>
<tr>
<td>ap7522</td>
<td>Filters out devices other than AP7522</td>
</tr>
<tr>
<td>ap7532</td>
<td>Filters out devices other than AP7532</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Filters out devices other than AP81XXs</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Filters out devices other than AP82XXs</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Filters out devices other than RFS4000s</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Filters out devices other than RFS6000s</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Filters out devices other than RFS7000s</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Filters out devices other than NX45XX series</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Filters out devices other than NX65XX series</td>
</tr>
</tbody>
</table>
nx75xx | Filters out devices other than NX75XX series
---|---
nx9000 | Filters out devices other than NX9000 series

**Examples**
rfs7000-37FABE(config)#device containing ap filter type ap71xx
% Error: Parsing cmd line (1)
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#device containing ap filter type ap650
rfs7000-37FABE(config-device-{'type': 'ap650', 'con}#

**Related Commands**

| no | Removes multiple devices from the network |
4.1.30 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.

Table 4.8 lists the command to enter the device categorization configuration mode.

<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 4-101</td>
</tr>
<tr>
<td>device-categorization-mode</td>
<td>Summarizes device categorization list configuration mode commands</td>
<td>page 4-102</td>
</tr>
</tbody>
</table>
4.30.1 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.

If a device categorization list does not exist, it is created.

Supported in the following platforms:
- Access Points — AP300, 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, 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
4.1.30.2 device-categorization-mode commands

Table 4.9 summarizes device categorization configuration 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 4-103</td>
</tr>
<tr>
<td>no</td>
<td>Removes a device from the device categorization list</td>
<td>page 4-104</td>
</tr>
</tbody>
</table>
4.1.30.2.1 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 — AP300, 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, 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**

- \(<1-1000>\): 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 neighboring 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 SSID.

**Note:** All APs are marked if no specific MAC address or SSID is provided.

- 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
4.1.30.2.2 no

device-categorization-mode commands

Removes a device from the device categorization list

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no mark-device <1-1000> [sanctioned|neighboring] [ap|client]
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 mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>|ssid <SSID> {mac <MAC>}}

<table>
<thead>
<tr>
<th>no mark-device</th>
<th>Removes a device from the marked devices list</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1000&gt;</td>
<td>Specify the mark device entry index.</td>
</tr>
<tr>
<td>sanctioned</td>
<td>Removes a device marked as sanctioned</td>
</tr>
<tr>
<td>neighboring</td>
<td>Removes a device marked as neighboring</td>
</tr>
<tr>
<td>ap</td>
<td>Removes a AP marked as sanctioned or neighboring based on its MAC address or SSID</td>
</tr>
<tr>
<td>{mac &lt;MAC&gt;}</td>
<td>• mac &lt;MAC&gt; – Optional. Specify the AP's MAC address.</td>
</tr>
<tr>
<td>ssid &lt;SSID&gt;}</td>
<td>• ssid &lt;SSID&gt; – Optional. Specify the AP's SSID. After specifying the SSID, you can optionally specify its MAC SSID.</td>
</tr>
</tbody>
</table>

- no mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}

<table>
<thead>
<tr>
<th>no mark-device</th>
<th>Removes a device from the marked devices list</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1000&gt;</td>
<td>Specify the mark device entry index.</td>
</tr>
<tr>
<td>sanctioned</td>
<td>Removes a wireless client marked as sanctioned</td>
</tr>
<tr>
<td>neighboring</td>
<td>Removes a wireless client marked as neighboring</td>
</tr>
<tr>
<td>client</td>
<td>Removes a wireless client marked as sanctioned or neighboring based on its MAC address</td>
</tr>
<tr>
<td>{mac &lt;MAC&gt;}</td>
<td>• mac &lt;MAC&gt; – Optional. Specify the wireless client’s MAC address.</td>
</tr>
</tbody>
</table>

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 |
4.1.31 dhcp-server-policy

Global Configuration Commands

Configures DHCP 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-server-policy <DHCP-POLICY-NAME>

Parameters

- dhcp-server-policy <DHCP-POLICY-NAME>

| <DHCP-POLICY-NAME> | Specify the DHCP 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 BOPT specific configuration
- dhcp-class Configure DHCP class (for address allocation using DHCP
  user-class options)
- dhcp-pool Configure DHCP server address pool
- 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.
4.1.32 dns-whitelist

Configures a DNS whitelist. A DNS whitelist is a list of domains allowed access to the network. Table 4.10 lists DNS Whitelist configuration mode commands.

Table 4.10 DNS-Whitelist Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-whitelist</td>
<td>Creates a DNS whitelist and enters its configuration mode</td>
<td>page 4-108</td>
</tr>
<tr>
<td>dns-whitelist-mode</td>
<td>Summarizes DNS whitelist configuration mode commands</td>
<td>page 4-109</td>
</tr>
</tbody>
</table>
4.1.32.1 dns-whitelist

Configures a DNS whitelist. A DNS whitelist is a list of domains allowed access to the network.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

dns-whitelist <DNS-WHITELIST-NAME>

Parameters
- dns-whitelist <DNS-WHITELIST-NAME>

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 |
4.1.32.2 dns-whitelist-mode commands

Table 4.11 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 4-110</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts to default</td>
<td>page 4-111</td>
</tr>
</tbody>
</table>
**4.1.32.2.1 permit**

- **dns-whitelist-mode commands**

A whitelist is a list of host names and IP addresses permitted access to the network or captive portal. This command adds a device by its hostname or IP address to the DNS whitelist.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit <IP/HOSTNAME> {suffix}
```

**Parameters**

- `permit <IP/HOSTNAME> {suffix}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP/HOSTNAME&gt;</code></td>
<td>Adds a device to the DNS whitelist</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP/HOSTNAME&gt;</code> — Specify the devices’ IP address or hostname.</td>
</tr>
<tr>
<td><code>suffix</code></td>
<td>Optional. Matches any hostname including the specified name as suffix</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-dns-whitelist-test)#permit company.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#
```

**Related Commands**

- `no` Removes a DNS whitelisted entry
4.1.32.2 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no permit <IP/HOSTNAME>
```

**Parameters**

- `no permit <IP/HOSTNAME>`

<table>
<thead>
<tr>
<th>&lt;IP/HOSTNAME&gt;</th>
<th>Removes a device from the DNS whitelist (identifies the device by its IP address or hostname)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP/HOSTNAME&gt;</code></td>
<td>Specified by the device's IP address or hostname.</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#permit company.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#

rfs7000-37FABE(config-dns-whitelist-test)#no permit company.com
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
rfs7000-37FABE(config-dns-whitelist-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>permit</th>
<th>Adds a device to the DNS whitelist</th>
</tr>
</thead>
</table>

4.1.33 end

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
end

Parameters
None

Examples
rfs7000-37FABE(config)#end
rfs7000-37FABE#
4.1.34 event-system-policy

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. Table 4.12 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 4-114</td>
</tr>
<tr>
<td>event-system-policy-mode</td>
<td>Summarizes event system policy configuration mode commands</td>
<td>page 4-115</td>
</tr>
</tbody>
</table>
4.1.34.1 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 administered 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
event-system-policy <EVENT-SYSTEM-POLICY-NAME>
```

Parameters

- `event-system-policy <EVENT-SYSTEM-POLICY-NAME>`

Examples

```
rfs7000-37FABE(config)#event-system-policy event-testpolicy
```

```
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#?
Event System Policy Mode commands:
et
geo
no

clears
commit
login
end
exit
help
revert
service
show
write
```

```
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#
```

Related Commands

```
no
```

Removes an event system policy
4.1.34.2 event-system-policy-mode commands

Table 4.13 summarizes event system policy configuration mode commands.

Table 4.13 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 4-116</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts to default</td>
<td>page 4-126</td>
</tr>
</tbody>
</table>
4.134.2.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog) [default|on|off]
```

The event types are:

```
aaa             AAA/Radius module
adv-wips       Adv-wips module
ap             Access Point module
captive-portal Captive Portal
cdp            Cisco Discovery Protocol
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
dwu            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 Configuration Daemon
radio          Radio module
rasst          Roaming-Assist module
smrt           Smart-rf module
smtpnot        Smtpnot module
system         System module
test           Test module
vrrp           Virtual Router Redundancy Protocol
wips           Wireless IPS module
```

**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**        | Configures 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  |
| **adv-wips**   | Configures advanced WIPS related event messages |
| **ap**         | Configures AP 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** | Configures 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  |

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>flex-log-access</td>
<td>Event flexible log access granted to client message</td>
</tr>
<tr>
<td>client-removed</td>
<td>Event client removed message</td>
</tr>
<tr>
<td>data-limit-exceed</td>
<td>Event client data limit exceed message</td>
</tr>
<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>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>
</tbody>
</table>

**certmgr**
- Configures certificate manager related event messages
  - ca-cert-actions-failure — Event CA certificate actions failure message
  - ca-cert-actions-success — Event CA certificate actions success message
  - ca-key-actions-failure — Event CA key actions failure message
  - ca-key-actions-success — Event CA key actions success message
  - cert-expiry — Event certificate expiry message
  - crl-actions-failure — Event Certificate Revocation List (CRL) actions failure message
  - crl-actions-success — Event CRL actions success message
  - csr-export-failure — Event CSR export failure message
  - csr-export-success — Event CSR export success message
  - delete-trustpoint-action — Event delete trustpoint action message
  - export-trustpoint — Event export trustpoint message
  - import-trustpoint — Event import trustpoint message
  - rsa-key-actions-failure — Event RSA key actions failure message
  - rsa-key-actions-success — Event RSA key actions success message
  - svr-cert-actions-success — Event server certificate actions success message
  - svr-cert-actions-failure — Event server certificate actions failure message

**certmgr-lite**
- Enables and configures logging of certificate manager (lite version) related event messages (applicable only to AP621, AP6521 and AP6511)

**cfgd**
- Configures configuration daemon module related event messages
  - acl-attached-altered — Event Access List (ACL) attached altered message
  - acl-rule-altered — Event ACL rule altered message

**cluster**
- Configures cluster module related messages
  - cmaster-cfg-update-fail — Event cluster master config update failed message
  - max-exceeded — Event maximum cluster count exceeded message

**crm**
- Configures Critical Resource Monitoring (CRM) related event messages
  - critical-resource-down — Event Critical Resource Down message
  - critical-resource-up — Event Critical Resource Up message
<table>
<thead>
<tr>
<th><code>&lt;event-type&gt;</code></th>
<th><code>&lt;event-name&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcpsvr</td>
<td>Configures 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>Configures 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-recovery – 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-recovery – 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>
</tbody>
</table>

Contd..
<table>
<thead>
<tr>
<th><strong>&lt;event-type&gt;</strong></th>
<th><strong>&lt;event-name&gt;</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>poe-state-change</td>
<td>Event PoE state change message</td>
</tr>
<tr>
<td>pwrsply-fail</td>
<td>Event failure of power supply message</td>
</tr>
<tr>
<td>raid-degraded</td>
<td>Event Redundant Array of Independent Disks (RAID) degraded message</td>
</tr>
<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>Configures 802.11 management module related event messages</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>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>unsanctioned-ap-active</td>
<td>Event unsanctioned AP active message</td>
</tr>
<tr>
<td>unsanctioned-ap-inactive</td>
<td>Event unsanctioned AP inactive message</td>
</tr>
<tr>
<td>unsanctioned-ap-status-change</td>
<td>Event unsanctioned AP status change</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>voice-call-failed</td>
<td>Event voice call failed message</td>
</tr>
<tr>
<td>wlan-time-access-disable</td>
<td>Event WLAN disabled by time-based-access message</td>
</tr>
<tr>
<td>wlan-time-access-enable</td>
<td>Event WLAN re-enabled by time-based-access message</td>
</tr>
<tr>
<td>wpa-wpa2-failed</td>
<td>Event WPA-WPA2 failed message</td>
</tr>
<tr>
<td>wpa-wpa2-key-rotn</td>
<td>Event WPA-WPA2 key rotn message</td>
</tr>
<tr>
<td>wpa-wpa2-success</td>
<td>Event WPA-WPA2 success 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>
| dot1x | Configures 802.1X authentication related event messages  
- dot1x-failed – Event EAP authentication failure message  
- dot1x-success – Event dot1x-success message |
| fwu | Configures firmware update (fwu) related event messages  
- fwuaborted – Event fwu aborted message  
- fwubadconfig – Event fwu aborted due to bad config message  
- fwucorruptedfile – Event fwu aborted due to corrupted file message  
- fwucouldntgetfile – Event fwu aborted because the system could not get file message  
- fwudone – Event fwu done message  
- fwufileundefined – Event fwu aborted due to file undefined message  
- fwunoneed – Event fwu no need message  
- fwuprodmismatch – Event fwu aborted due to product mismatch message  
- fwuserverundefined – Event fwu aborted due to server undefined message  
- fwuserverunreachable – Event fwu aborted due to server unreachable message  
- fwusignmismatch – Event fwu aborted due to signature mismatch message  
- fwusyserr – Event fwu aborted due to system error message  
- fwusupportedhwnd – Event fwu aborted due to unsupported hardware message  
- fwusupportedmodelnum – Event fwu aborted due to unsupported FIPS model number message  
- fwuvermismatch – Event fwu aborted due to version mismatch message |
| isdn | Configures file Integrated Service Digital Network (ISDN) module related event messages  
- isdn-alert – Event ISDN alert message  
- isdn-crit – Event ISDN critical message  
- isdn-debug – Event ISDN debug message  
- isdn-emerg – Event ISDN emergency message  
- isdn-err – Event ISDN error message  
- isdn-info – Event ISDN info message  
- isdn-notice – Event ISDN notice message  
- isdn-warning – Event ISDN warning message |
| l2tpv3 | Configures L2TPv3 related event messages  
- l2tpv3-tunnel-down – Event L2TPv3 tunnel down message  
- l2tpv3-tunnel-up – Event L2TPv3 tunnel up message |
| licmgr | Configures license manager module related event messages  
- lic-installed-count – Event total number of license installed count message  
- lic-installed-default – Event default license installation message  
- lic-installed – Event license installed message  
- lic-invalid – Event license installation failed message  
- lic-removed – Event license removed message |
<table>
<thead>
<tr>
<th><code>&lt;event-type&gt;</code></th>
<th><code>&lt;event-name&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mgmt</strong></td>
<td>Configures 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><strong>mesh</strong></td>
<td>Configures 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><strong>nsm</strong></td>
<td>Configures <em>Network Service Module</em> (NSM) related event message</td>
</tr>
<tr>
<td></td>
<td>• dhcpc-err – Event DHCP certification error message</td>
</tr>
<tr>
<td></td>
<td>• dhcpdefr – Event DHCP defr message</td>
</tr>
<tr>
<td></td>
<td>• dhcpip – Event DHCP IP message</td>
</tr>
<tr>
<td></td>
<td>• dhcpipchg – 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>• dhcplsexp – 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>• dhcnodef – 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><strong>&lt;event-type&gt;</strong></td>
<td><strong>&lt;event-name&gt;</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| pm | Configures process monitor module related event messages  
• procid – Event proc ID message  
• procmxrst – Event proc max restart message  
• procnoresp – Event proc no response message  
• procrst – Event proc restart message  
• procsrt – Event proc start message  
• procspsstop – Event proc stop message  
• procsysrst – Event proc system restart message  
• startupcomplete – Event startup complete message |
| radconf | Configures 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 | Configures 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 |
| smrt | Configures 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  
• root-recovery – Event meshpoint root recovery message |
<table>
<thead>
<tr>
<th><code>&lt;event-type&gt;</code></th>
<th><code>&lt;event-name&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>smtpnot</td>
<td>Configures 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>Configures 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>• 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>• procstop – 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>• 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>
</tbody>
</table>
### Examples

```bash
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)#
```

```bash
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

| `no` | Resets or disables event monitoring |
4.1.34.2.2 no

Negates an event monitoring configuration

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no event <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog] [default|on|off]
```

**Parameters**

- no event <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog] [default|on|off]

<table>
<thead>
<tr>
<th>no event &lt;EVENT-TYPE&gt; &lt;EVENT-NAME&gt;</th>
<th>Removes the specified event monitoring activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;EVENT-TYPE&gt; — Select the event type.</td>
<td></td>
</tr>
<tr>
<td>&lt;EVENT-NAME&gt; — After selecting the event type, specify the event name.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The system stops network monitoring for the occurrence of the specified event and no notification is sent if the event occurs.

**Examples**

```plaintext
rfs7000-37FABE(config-event-system-policy-TestPolicy)#event ap adopted syslog default
rfs7000-37FABE(config-event-system-policy-TestPolicy)#

rfs7000-37FABE(config-event-system-policy-TestPolicy)#no event ap adopted syslog
rfs7000-37FABE(config-event-system-policy-TestPolicy)#
```

**Related Commands**

- `event` Configures the action taken for each event
4.1.35 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 — AP300, 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, 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
- `clump` 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
- `logging` Firewall enhanced logging
- `no` Negate a command or set its defaults
- `proxy-arp` Enable generation of ARP responses 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)

```
clrscr
commit
do
end
exit
help
revert
service
show
write
```

```
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>Removes an existing firewall policy</td>
</tr>
</tbody>
</table>

**NOTE:** For more information on Firewall policy, see *Chapter 13, FIREWALL-POLICY.*
4.1.36 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
global-association-list <GLOBAL-ASSOC-LIST-NAME>
```

Parameters

- `global-association-list <GLOBAL-ASSOC-LIST-NAME>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</td>
<td>Specify the global association list name. If a list with the same name does not exist, it is created. <strong>Note</strong>: 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. <strong>Note</strong>: 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.</td>
</tr>
</tbody>
</table>

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 return 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
```

```
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)#

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-global-assoc-list-my-clients)#

rfs4000-229D58(config)#show context

............................
global-association-list test
  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)#

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)#
4.1.37 **host**

*Global Configuration Commands*

Enters the configuration context of a remote device using its hostname

Supported in the following platforms:

- Access Points — AP300, 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, 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)#
```
4.1.38 **inline-password-encryption**

- **Global Configuration Commands**

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 — AP300, 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, 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)#
```

```
rfs7000-37FABE(config)#commit wr mem
rfs7000-37FABE(config)#
```

This command uses the specified password for encryption key and stores it outside of startup-config

```
rfs7000-37FABE(config)#inline-password-encryption
rfs7000-37FABE(config)#
```

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>
</tbody>
</table>
4.1.39 ip

- **Global Configuration Commands**

Configures IP access control lists

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ip access-list <IP-ACCESS-LIST-NAME>
```

**Parameters**

- `ip access-list <IP-ACCESS-LIST-NAME>`

| access-list | Configures an IP access list |
| <IP-ACCESS-LIST-NAME> | • `<IP-ACCESS-LIST-NAME>` — Specify the ACL name. If the access list does not exist, it is created. |

**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
- 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-ip-acl-test)#
```

**Related Commands**

- `no` Removes an IP access control list

**NOTE:** For more information on access control lists, see *Chapter 11, ACCESS-LIST.*
4.1.40 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 — AP300, 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, 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
- failover-delay
- force-l2-path-recovery
- hello-interval
- no
- reconnect-attempts
- reconnect-interval
- retry-attempts
- retry-interval
- rx-window-size
- tx-window-size
- clrscr
- commit
- end
- exit
- help
- revert
- service
- show

Configures an L2TPv3 tunnel policy

- <L2TPV3-POLICY-NAME> — Specify a policy name. The policy is created if it does not exist. To modify an existing L2TPv3, specify its name.
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 23, L2TPV3-POLICY.*
4.1.41 mac

Global Configuration Commands

Configures MAC access control lists

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

mac access-list <MAC-ACCESS-LIST-NAME>

Parameters

- mac access-list <MAC-ACCESS-LIST-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.
4.1.42 management-policy

Configures a management policy. Management policies include services that run on a device, welcome messages, banners etc.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
management-policy <MANAGEMENT-POLICY-NAME>

Parameters
- management-policy <MANAGEMENT-POLICY-NAME>

Examples
rfs7000-37FABE(config)#management-policy test
rfs7000-37FABE(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)
- 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
- 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

rfs7000-37FABE(config-management-policy-test)#

Related Commands
- no Removes an existing management policy

NOTE: For more information on Management policy configuration, see Chapter 16, MANAGEMENT-POLICY.
4.1.43 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

meshpoint [<MESHPOINT-NAME>|containing <WORD>]

Parameters

- meshpoint [<MESHPOINT-NAME>|containing <WORD>]
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MESHPOINT-NAME&gt;</td>
<td>Specify the meshpoint name. If the meshpoint does not exist, it is created.</td>
</tr>
<tr>
<td>containing &lt;WORD&gt;</td>
<td>Selects existing meshpoints containing the sub-string &lt;WORD&gt; in their names</td>
</tr>
</tbody>
</table>

Examples

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
- 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 Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
desc End current mode and change to EXEC mode
desc End current mode and down to previous mode
desc 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-TestMeshpoint)#

Related Commands

- no Removes an existing meshpoint

NOTE: For more information on Meshpoint configuration, see Chapter 27, MESHPOINT
### 4.1.44 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** — AP300, 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, 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
commit
end
exit
help
revert
service
show
write
```

**Related Commands**

```
no
```

Removes an existing meshpoint QoS policy

**NOTE:** For more information on Meshpoint QoS policy configuration, see *Chapter 27, MESHPOINT*
4.1.45 mint-policy

Global Configuration Commands

Configures the global MiNT policy

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

mint-policy global-default

Parameters

- mint-policy global-default

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global-default</td>
<td>Uses the global default MiNT policy</td>
</tr>
</tbody>
</table>

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
del End current mode and change to EXEC mode
help Description of the interactive help system
revert Revert changes
show Service Commands
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 15, MiNT-POLICY.
4.1.46 nac-list

A Network Access Control (NAC) policy configures a list of devices that can access a network based on their MAC addresses. Table 4.14 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 4-142</td>
</tr>
<tr>
<td>nac-list-mode commands</td>
<td>Summarizes NAC list configuration mode commands</td>
<td>page 4-143</td>
</tr>
</tbody>
</table>
4.1.46.1 nac-list

Configures a NAC list that manages access to the network

Supported in the following platforms:
- Access Points — AP300, 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, 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
### 4.1.46.2 nac-list-mode commands

- **nac-list**

  Table 4.15 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 4-144</td>
</tr>
<tr>
<td>include</td>
<td>Specifies the MAC addresses included in the NAC enforcement list</td>
<td>page 4-145</td>
</tr>
<tr>
<td>no</td>
<td>Cancels an exclude or include NAC list rule</td>
<td>page 4-146</td>
</tr>
</tbody>
</table>
4.1.46.2.1 exclude

nac-list-mode commands

Specifies the MAC addresses excluded from the NAC enforcement list

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]

Parameters

- exclude <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 exclude from the NAC enforcement list&lt;br&gt;&lt;ul&gt;&lt;li&gt;&lt;START-MAC&gt; — Specify the first MAC address in the range.&lt;br&gt;&lt;strong&gt;Note:&lt;/strong&gt; Use this parameter to specify a single MAC address.&lt;/li&gt;&lt;/ul&gt;</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)&lt;br&gt;&lt;ul&gt;&lt;li&gt;&lt;END-MAC&gt; — Specify the last MAC address in the range.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>precedence &lt;1-1000&gt;</td>
<td>Sets the rule precedence. Exclude entries are checked in the order of their rule precedence.&lt;br&gt;&lt;ul&gt;&lt;li&gt;&lt;1-1000&gt; — Specify a value from 1 - 1000.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
</tbody>
</table>

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)#
```
4.1.46.2.2 include

nac-list-mode commands

Specifies the MAC addresses included in the NAC enforcement list

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

\[ \text{include } \text{<START-MAC> [\text{<END-MAC> precedence } \text{<1-1000>}]} \]

Parameters

- \text{include } \text{<START-MAC> [\text{<END-MAC> precedence } \text{<1-1000>}]}

| \text{<START-MAC>} | Specifies a range of MAC addresses or a single MAC address to include in the NAC enforcement list  
\|---|---|
| \text{<END-MAC>} | Specifies the last MAC address in the range (optional if a single MAC is added to the list)  
\|---|---|
| \text{precedence } \text{<1-1000>} | Sets the rule precedence. Include entries are checked in the order of their rule precedence.  
\|---|---|

Note: Use this parameter to specify a single MAC address

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
\text{exclude } 00-04-96-BA-2A 00-04-96-BA-2A precedence 1
\text{include } 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
rfs7000-37FABE(config-nac-list-test)#
4.1.46.2.3 no

nac-list-mode commands

Cancels an exclude or include NAC list rule

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [exclude|include]

no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]

Parameters

- no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]

<table>
<thead>
<tr>
<th>no exclude</th>
<th>Removes an exclude rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>no include</td>
<td>Removes an include rule</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;START-MAC&gt;</th>
<th>Specifies a range of MACs included in/removed from the NAC enforcement list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the first MAC address in the range.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use this parameter to specify a single MAC address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;END-MAC&gt;</th>
<th>Specify the last MAC address in the range (optional if a single MAC is added to the list).</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>precedence &lt;1-1000&gt;</th>
<th>Sets the rule precedence for this rule. Exclude or include entries are checked in the order of their rule precedence.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-1000&gt; — Specify a value from 1 - 1000.</td>
</tr>
</tbody>
</table>

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>
4.1.47 no

Negates a command, or reverts configured settings to their default

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```


no [ap300|ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]

no client-identity <CLIENT-IDENTITY-NAME>
no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>

no device {containing <WORD>} {{filter type [ap621|ap622|ap650|ap6511|ap6521|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|nx45xx|nx65xx|nx75xx|nx9000]}}


no password-encryption secret 2 <OLD-PASSPHRASE>

no profile {ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|nx45xx|nx65xx|nx75xx|nx9000]

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 NX45XX, NX65XX, NX9000 series service platforms:
no smart-cache-policy <SMART-CACHE-POLICY-NAME>
The following ‘no’ command is specific to the NX45XX and NX65XX series service platforms:
no url-list <URL-LIST-NAME>
**Parameters**


<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no aaa-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Deletes the specified AAA policy</td>
</tr>
<tr>
<td>no aaa-tacacs-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Deletes the specified AAA TACACS policy</td>
</tr>
<tr>
<td>no auto-provisioning-policy <code>&lt;POLICY-NAME&gt;</code></td>
<td>Deletes the specified auto provisioning policy</td>
</tr>
</tbody>
</table>
| no bonjour-gw-discovery-policy `<POLICY-NAME>` | Deletes the specified Bonjour GW discovery policy  
**Note:** This feature is supported only on RFS7000 and AP7131. |
| no bonjour-gw-forwarding-policy `<POLICY-NAME>` | Deletes the specified Bonjour GW forwarding policy  
**Note:** This feature is supported only on RFS7000 and AP7131. |
<p>| no captive-portal <code>&lt;CAPTIVE-PORTAL-NAME&gt;</code> | Deletes the specified captive portal |
| no device-categorization <code>&lt;DEVICE-CATEGORIZATION-LIST-NAME&gt;</code> | Deletes the specified device categorization list |
| no dhcp-server-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified DHCP server policy |
| no dns-whitelist <code>&lt;DNS-WHITELIST-NAME&gt;</code> | Deletes the specified DNS Whitelist |
| no event-system-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified event system policy |
| no firewall-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified firewall policy |
| no global-association-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified global association policy |
| no inline-password-encryption | Disables storing of the encryption key in the startup configuration file |
| no ip access-list <code>&lt;IP-ACCESS-LIST-NAME&gt;</code> | Deletes the specified IP access list |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| no l2tpv3 policy `<L2TPV3-POLICY-NAME>` | Deletes the specified L2TPv3 policy  
**Note:** The default L2TPv3 policy cannot be deleted. |
<p>| no mac access-list <code>&lt;MAC-ACCESS-LIST-NAME&gt;</code> | Deletes the specified MAC access list |
| no management-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified management policy |
| no meshpoint <code>&lt;MESHPOINT-NAME&gt;</code> | Deletes the specified meshpoint |
| no meshpoint-qos-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified meshpoint QoS policy |
| no nac-list <code>&lt;NAC-LIST-NAME&gt;</code> | Deletes the specified NAC list |
| no passpoint-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified passpoint policy |
| no radio-qos-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified radio QoS policy |
| no radius-group <code>&lt;RADIANUS-GROUP-NAME&gt;</code> | Deletes the specified RADIUS group |
| no radius-server-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified RADIUS server policy |
| no radius-user-pool-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified RADIUS user pool policy |
| no rf-domain <code>&lt;RF-DOMAIN-NAME&gt;</code> | Deletes the specified RF Domain |
| no role-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified role policy |
| no routing-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified routing policy |
| no smart-rf-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified smart RF policy |
| no wips-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified WIPS policy |
| no wlan-qos-policy <code>&lt;POLICY-NAME&gt;</code> | Deletes the specified WLAN QoS policy |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no alias</td>
<td>Removes an existing network, VLAN, or service alias. Select the alias type. The options are: network, vlan, and service.</td>
</tr>
<tr>
<td>address-range &lt;ADDRESS-RANGE-ALIAS-NAME&gt;</td>
<td>Deletes the specified address range alias</td>
</tr>
<tr>
<td>host &lt;HOST-ALIAS-NAME&gt;</td>
<td>Deletes the specified host alias</td>
</tr>
<tr>
<td>network &lt;NETWORK-ALIAS-NAME&gt;</td>
<td>Deletes the specified network alias</td>
</tr>
<tr>
<td>network-group &lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>Removes the specified component (IP address(es), hosts, or network address(es)) of the specified network-group alias</td>
</tr>
<tr>
<td>network-service &lt;NETWORK-SERVICE-ALIAS-NAME&gt;</td>
<td>Deletes the specified network-service alias</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ALIAS-NAME&gt;</td>
<td>Removes the VLAN alias identified by the &lt;VLAN-ALIAS-NAME&gt; keyword</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no [ap300</td>
<td>ap621</td>
</tr>
<tr>
<td>no ap300</td>
<td>Removes an AP300 from the network</td>
</tr>
<tr>
<td>no ap621</td>
<td>Removes an AP621 from the network</td>
</tr>
<tr>
<td>no ap622</td>
<td>Removes an AP622 from the network</td>
</tr>
<tr>
<td>no ap650</td>
<td>Removes an AP650 from the network</td>
</tr>
<tr>
<td>no ap6511</td>
<td>Removes an AP6511 from the network</td>
</tr>
<tr>
<td>no ap6521</td>
<td>Removes an AP6521 from the network</td>
</tr>
<tr>
<td>no ap6522</td>
<td>Removes an AP6522 from the network</td>
</tr>
<tr>
<td>no ap6532</td>
<td>Removes an AP6532 from the network</td>
</tr>
<tr>
<td>no ap6562</td>
<td>Removes an AP6562 from the network</td>
</tr>
<tr>
<td>no ap71xx</td>
<td>Removes an AP71XX from the network</td>
</tr>
<tr>
<td>no ap7502</td>
<td>Removes an AP7502 from the network</td>
</tr>
<tr>
<td>no ap7522</td>
<td>Removes an AP7522 from the network</td>
</tr>
<tr>
<td>np ap7532</td>
<td>Removes an AP7532 from the network</td>
</tr>
<tr>
<td>no ap81xx</td>
<td>Removes an AP81XX from the network</td>
</tr>
</tbody>
</table>
### GLOBAL CONFIGURATION COMMANDS

<table>
<thead>
<tr>
<th>No Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ap82xx</td>
<td>Removes an AP82XX from the network</td>
</tr>
<tr>
<td>no rfs4000</td>
<td>Removes a RFS4000 from the network</td>
</tr>
<tr>
<td>no rfs6000</td>
<td>Removes a RFS6000 from the network</td>
</tr>
<tr>
<td>no rfs7000</td>
<td>Removes a RFS7000 from the network</td>
</tr>
<tr>
<td>no nx45xx</td>
<td>Removes a NX45XX series device from the network</td>
</tr>
<tr>
<td>no nx65xx</td>
<td>Removes a NX65XX series device from the network</td>
</tr>
<tr>
<td>no nx75xx</td>
<td>Removes a NX75XX series device from the network</td>
</tr>
<tr>
<td>no nx9000</td>
<td>Removes a NX9000 series device from the network</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Identifies the device to remove by its MAC address</td>
</tr>
<tr>
<td>no client-identity &lt;CLIENT-IDENTITY-NAME&gt;</td>
<td>Removes the set of client identity fingerprints identified by the &lt;CLIENT-NAME&gt; keyword</td>
</tr>
<tr>
<td>no client-identity-group &lt;CLIENT-IDENTITY-GROUP-NAME&gt;</td>
<td>Removes the client identity group identified by the &lt;CLIENT-IDENTITY-GROUP-NAME&gt; keyword</td>
</tr>
<tr>
<td>no device {containing &lt;WORD&gt;} {{filter type [ap621</td>
<td>ap622</td>
</tr>
<tr>
<td>no device containing &lt;WORD&gt;</td>
<td>Optional. Removes devices with hostname containing the substring specified by the &lt;WORD&gt; keyword</td>
</tr>
<tr>
<td>filter type &lt;DEVICE-TYPE&gt;</td>
<td>Optional. Filters devices based on the device type selected</td>
</tr>
<tr>
<td>no passwod-encryption secret 2 &lt;OLD-PASSPHRASE&gt;</td>
<td>Enables password encryption</td>
</tr>
</tbody>
</table>
- **no profile** {ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|containing|filter|nx54xx|nx65xx|nx75xx|nx9000} `<PROFILE-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no profile</td>
<td>Removes a profile and its associated configurations</td>
</tr>
<tr>
<td>ap621</td>
<td>Optional. Removes a AP621 profile</td>
</tr>
<tr>
<td>ap622</td>
<td>Optional. Removes a AP622 profile</td>
</tr>
<tr>
<td>ap650</td>
<td>Optional. Removes a AP650 profile</td>
</tr>
<tr>
<td>ap6511</td>
<td>Optional. Removes a AP6511 profile</td>
</tr>
<tr>
<td>ap6521</td>
<td>Optional. Removes a AP6521 profile</td>
</tr>
<tr>
<td>ap6522</td>
<td>Optional. Removes a AP6522 profile</td>
</tr>
<tr>
<td>ap6532</td>
<td>Optional. Removes a AP6532 profile</td>
</tr>
<tr>
<td>ap6562</td>
<td>Optional. Removes a AP6562 profile</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Optional. Removes a AP71XX profile</td>
</tr>
<tr>
<td>ap7502</td>
<td>Optional. Removes a AP7502 profile</td>
</tr>
<tr>
<td>ap7522</td>
<td>Optional. Removes a AP7522 profile</td>
</tr>
<tr>
<td>ap7532</td>
<td>Optional. Removes a AP7532 profile</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Optional. Removes a AP81XX profile</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Optional. Removes a AP82XX profile</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Optional. Removes a RFS4000 profile</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Optional. Removes a RFS6000 profile</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Optional. Removes a RFS7000 profile</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Optional. Removes a NX45XX profile</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Optional. Removes a NX65XX profile</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Optional. Removes a NX75XX profile</td>
</tr>
<tr>
<td>nx9000</td>
<td>Optional. Removes a NX9000 series profile</td>
</tr>
<tr>
<td><code>&lt;PROFILE-NAME&gt;</code></td>
<td>Specifies the profile name</td>
</tr>
</tbody>
</table>

- **no wlan** [<WLAN-NAME>|all|containing `<WLAN-NAME-SUBSTRING>`]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no wlan</td>
<td>Removes a WLAN</td>
</tr>
<tr>
<td><code>&lt;WLAN-NAME&gt;</code></td>
<td>Identifies the WLAN name</td>
</tr>
<tr>
<td>all</td>
<td>Removes all WLANs</td>
</tr>
<tr>
<td>containing <code>&lt;WLAN-NAME-SUBSTRING&gt;</code></td>
<td>Removes WLANs whose names contain the string specified by the <code>&lt;WLAN-NAME-SUBSTRING&gt;</code> parameter</td>
</tr>
</tbody>
</table>
**GLOBAL CONFIGURATION COMMANDS 4 - 153**

- `no service set [command-history|reboot-history|upgrade-history] {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no service set</code></td>
<td>Resets service command parameters</td>
</tr>
<tr>
<td><code>command-history</code></td>
<td>Resets command history file size to default (200)</td>
</tr>
<tr>
<td><code>reboot-history</code></td>
<td>Resets reboot history file size to default (50)</td>
</tr>
<tr>
<td><code>upgrade-history</code></td>
<td>Resets upgrade history file size to default (50)</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Resets service command parameters on a specified device</td>
</tr>
</tbody>
</table>

- `no smart-cache-policy <POLICY-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no smart-cache-policy</code></td>
<td>Deletes the specified smart content cache policy</td>
</tr>
<tr>
<td><code>&lt;POLICY-NAME&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This command is specific to the NX45XX, NX65XX, and NX9000 series service platforms.

- `no url-list <URL-LIST-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no url-list</code></td>
<td>Deletes the specified URL list</td>
</tr>
<tr>
<td><code>&lt;URL-LIST-NAME&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This command is specific to the NX45XX and NX65XX series service platforms.

**Examples**

```bash
rfs7000-37FABE(config)#no ?
aaa-policy                   Delete a aaa policy
aaa-tacacs-policy            Delete a aaa tacacs policy
alias                        Alias
ap300                        Delete an AP300
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
ap7502                       Delete an AP7502 access point
ap7522                       Delete an AP7522 access point
ap7532                       Delete an AP7532 access point
ap71xx                       Delete an AP71XX access point
ap81xx                       Delete an AP81XX access point
ap82xx                       Delete an AP82XX access point
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
captive-portal              Delete a captive portal
client-identity              Client identity (DHCP Device Fingerprinting)
client-identity-group        Client identity group (DHCP Fingerprint Database)
customize                    Restore the custom cli commands to default
device                       Delete multiple devices
device-categorization        Delete device categorization object
dhcp-server-policy           DHCP server policy
dns-whitelist                Delete a whitelist object
event-system-policy          Delete a event system policy
firewall-policy              Configure 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)
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
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
rfs5000                     Delete an RFS5000 wireless controller
rfs7000                     Delete an RFS7000 wireless controller
role-policy                 Role based firewall policy
routing-policy              Policy Based Routing Configuration
smart-rf-policy             Delete a smart-rf-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
rfs7000-37FABE(config)#
nx9500-6C8809(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                    AP7502 access point profile
  ap7522                    AP7522 access point profile
  ap7532                    AP7532 access point profile
  ap81xx                    Delete an AP81XX access point
  ap82xx                    Delete an AP82XX access point
  association-acl-policy    Delete an association-acl policy
  auto-provisioning-policy  Delete an auto-provisioning policy
  captive-portal            Delete a captive portal
  client-identity           Client identity (DHCP Device Fingerprinting)
  client-identity-group    Client identity group (DHCP Fingerprint Database)
  customize                 Restore the custom cli commands to default
  device                    Delete multiple devices
device-categorization      Delete device categorization object
dhcp-server-policy         DHCP server policy
dns-whitelist               Delete a whitelist object
event-system-policy        Delete a event system policy
firewall-policy             Configure firewall 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)
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
nx45xx                      Delete an NX45XX integrated services platform
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
rfs4000                     Delete an RFS4000 wireless controller
rfs6000                     Delete an RFS6000 wireless controller
rfs7000                     Delete an RFS7000 wireless controller
role-policy                Role based firewall policy
routing-policy             Policy Based Routing Configuration
smart-cache-policy         Delete a content caching
smart-rf-policy            Delete a smart-rf-policy
url-list                   Delete a URL list
wips-policy                Delete a wips policy
wlan                       Delete a wlan object
wlan-qos-policy            Delete a wireless lan QoS configuration policy
service                    Service Commands

nx9500-6C8809(config)#
### 4.1.48 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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)#?
rfs4000-229D58(config-passpoint-policy-test)#?
```

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
- `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

```
rfs4000-229D58(config-passpoint-policy-test)#
```

**Related Commands**

- `no` Removes an existing passpoint policy
NOTE: For more information on passpoint policy, see Chapter 28, PASSPOINT POLICY.
4.1.49 password-encryption

- **Global Configuration Commands**

Enables password encryption

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
password-encryption secret 2 <LINE>
```

**Parameters**

- `password-encryption 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 company
rfs7000-37FABE(config)#
```

```
nx6500-31FABE(config)#password-encryption secret 2 test
nx6500-31FABE(config)#
```

**Related Commands**

| no | Disables password encryption |
4.1.50 profile

Global Configuration Commands

Configures profile related commands. If no parameters are given, all profiles are selected.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
profile {ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap71xx|ap81xx|ap82xx|containing|filter|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000}
```

```
profile {ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000}
<DEVICE-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|nx65xx|nx75xx|nx9000]}
```

```
profile {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]}
```

Parameters

- `profile {ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|containing|filter|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000} <DEVICE-PROFILE-NAME>`

<table>
<thead>
<tr>
<th>profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap621</td>
<td>Optional. Configures AP621 profile commands</td>
</tr>
<tr>
<td>ap622</td>
<td>Optional. Configures AP622 profile commands</td>
</tr>
<tr>
<td>ap650</td>
<td>Optional. Configures AP650 profile commands</td>
</tr>
<tr>
<td>ap6511</td>
<td>Optional. Configures AP6511 profile commands</td>
</tr>
<tr>
<td>ap6521</td>
<td>Optional. Configures AP6521 profile commands</td>
</tr>
<tr>
<td>ap6522</td>
<td>Optional. Configures AP6522 profile commands</td>
</tr>
<tr>
<td>ap6532</td>
<td>Optional. Configures AP6532 profile commands</td>
</tr>
<tr>
<td>ap6562</td>
<td>Optional. Configures AP6562 profile commands</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Optional. Configures AP71XX profile commands</td>
</tr>
<tr>
<td>ap7502</td>
<td>Optional. Configures AP7502 profile commands</td>
</tr>
<tr>
<td>ap7522</td>
<td>Optional. Configures AP7522 profile commands</td>
</tr>
<tr>
<td>ap7532</td>
<td>Optional. Configures AP7532 profile commands</td>
</tr>
</tbody>
</table>
profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]}

- profile {containing <DEVICE-PROFILE-NAME>}  Optional. Configures device profile commands
- containing <DEVICE-PROFILE-NAME>  Optional. Configures profiles that contain a specified sub-string in the hostname
  - <DEVICE-PROFILE-NAME> – Specify a sub-string in the profile name to filter profiles.
- 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:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap621</td>
<td>Optional. Selects an AP621 profile</td>
</tr>
<tr>
<td>ap622</td>
<td>Optional. Selects an AP622 profile</td>
</tr>
<tr>
<td>ap650</td>
<td>Optional. Selects an AP650 profile</td>
</tr>
<tr>
<td>ap6511</td>
<td>Optional. Selects an AP6511 profile</td>
</tr>
<tr>
<td>ap6521</td>
<td>Optional. Selects an AP6521 profile</td>
</tr>
<tr>
<td>ap6522</td>
<td>Optional. Selects an AP6522 profile</td>
</tr>
<tr>
<td>ap6532</td>
<td>Optional. Selects an AP6532 profile</td>
</tr>
<tr>
<td>ap6562</td>
<td>Optional. Selects an AP6562 profile</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Optional. Selects an AP71XX profile</td>
</tr>
<tr>
<td>ap7502</td>
<td>Optional. Selects an AP7502 profile</td>
</tr>
<tr>
<td>ap7522</td>
<td>Optional. Selects an AP7522 profile</td>
</tr>
<tr>
<td>ap7532</td>
<td>Optional. Selects an AP7532 profile</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Optional. Selects an AP81XX profile</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>profile</strong></td>
<td>Configures device profile commands</td>
</tr>
<tr>
<td><strong>filter type</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• type – Filters profiles by the device type. Select a device type from the following options:</td>
</tr>
<tr>
<td>ap621</td>
<td>Optional. Selects an AP621 profile</td>
</tr>
<tr>
<td>ap622</td>
<td>Optional. Selects an AP622 profile</td>
</tr>
<tr>
<td>ap650</td>
<td>Optional. Selects an AP650 profile</td>
</tr>
<tr>
<td>ap6511</td>
<td>Optional. Selects an AP6511 profile</td>
</tr>
<tr>
<td>ap6521</td>
<td>Optional. Selects an AP6521 profile</td>
</tr>
<tr>
<td>ap6522</td>
<td>Optional. Selects an AP6522 profile</td>
</tr>
<tr>
<td>ap6532</td>
<td>Optional. Selects an AP6532 profile</td>
</tr>
<tr>
<td>ap6562</td>
<td>Optional. Selects an AP6562 profile</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Optional. Selects an AP71XX profile</td>
</tr>
<tr>
<td>ap7502</td>
<td>Optional. Selects an AP7502 profile</td>
</tr>
<tr>
<td>ap7522</td>
<td>Optional. Selects an AP7522 profile</td>
</tr>
<tr>
<td>ap7532</td>
<td>Optional. Selects an AP7532 profile</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Optional. Selects an AP81XX profile</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Optional. Selects an AP82XX profile</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Optional. Selects a RFS4000 profile</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Optional. Selects a RFS6000 profile</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Optional. Selects a RFS7000 profile</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Optional. Selects a NX45XX series profile</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Optional. Selects a NX65XX profile</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Optional. Selects a NX75XX profile</td>
</tr>
<tr>
<td>nx9000</td>
<td>Optional. Selects a NX9000 series profile</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#?

Profile Mode commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopter-auto-provisioning-poly-rule-lookup</td>
<td>Use centralized auto-provisioning policy when adopted by another controller</td>
</tr>
<tr>
<td>alias</td>
<td>Alias</td>
</tr>
<tr>
<td>ap300</td>
<td>Adopt/unadopt AP300 device to this profile/device</td>
</tr>
<tr>
<td>area</td>
<td>Set name of area where the system is located</td>
</tr>
<tr>
<td>arp</td>
<td>Address Resolution Protocol (ARP)</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enable learning network configuration of the devices that come for adoption</td>
</tr>
<tr>
<td>autogen-uniqueid</td>
<td>Autogenerate a unique id</td>
</tr>
<tr>
<td>autinstall</td>
<td>Autoinstall settings</td>
</tr>
<tr>
<td>bridge</td>
<td>Ethernet bridge</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Captive portal</td>
</tr>
<tr>
<td>cdp</td>
<td>Cisco Discovery Protocol</td>
</tr>
<tr>
<td>cluster</td>
<td>Cluster configuration</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enable persistence of configuration across reloads (startup config file)</td>
</tr>
<tr>
<td>controller</td>
<td>WLAN controller configuration</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Critical Resource</td>
</tr>
<tr>
<td>crypto</td>
<td>Encryption related commands</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Device firmware upgrade</td>
</tr>
<tr>
<td>dot1x</td>
<td>802.1X</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configure IP DSCP to 802.1p priority mapping for untagged frames</td>
</tr>
<tr>
<td>email-notification</td>
<td>Email notification configuration</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Check the firmware versions of devices before interoperating</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Environmental Sensors Configuration</td>
</tr>
<tr>
<td>events</td>
<td>System event messages</td>
</tr>
<tr>
<td>export</td>
<td>Export a file</td>
</tr>
<tr>
<td>floor</td>
<td>Set the floor within a area where the system is located</td>
</tr>
<tr>
<td>gre</td>
<td>GRE protocol</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Specify HTTP-Analysis configuration</td>
</tr>
<tr>
<td>interface</td>
<td>Select an interface to configure</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>L2tpv3 protocol</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>L3e lite Table</td>
</tr>
<tr>
<td>led</td>
<td>Turn LEDs on/off on the device</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Enable device firmware to auto downgrade when other legacy devices are detected</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto upgrade of legacy devices</td>
</tr>
<tr>
<td>lldp</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configure load balancing parameter</td>
</tr>
<tr>
<td>logging</td>
<td>Modify message logging facilities</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>MAC Address Table</td>
</tr>
<tr>
<td>mac-auth</td>
<td>802.1X</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Memory profile to be used on the device</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configure meshpoint device parameters</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configure meshpoint monitoring</td>
</tr>
</tbody>
</table>
min-misconfiguration-recovery-time       Check controller connectivity after configuration is received
mint                                     MiNT protocol
misconfiguration-recovery-time           Check controller connectivity after configuration is received
neighbor-inactivity-timeout             Configure neighbor inactivity timeout
neighbor-info-interval                   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
reevaluate-everytime                    Set the flag to reevaluate autoprovisioning policy everytime
remove-override                          Remove configuration item override from the device (so profile value takes effect)
rf-domain-manager                        RF Domain Manager
router                                   Dynamic routing
spanning-tree                            Spanning tree
tunnel-controller                       Tunnel Controller group this controller belongs to
use                                      Set setting to use
vrrp                                     VRRP configuration
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

rfs7000-37FABE(config-profile-default-rfs7000)#
nx4500-5CFA2B(config-profile-test)#?
Profile Mode commands:
  adopter-auto-provisioning-policy-lookup Use centralized auto-provisioning policy when adopted by another controller
  alias                                   Alias
  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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoinstall</td>
<td>Autoinstall settings</td>
</tr>
<tr>
<td>bridge</td>
<td>Ethernet bridge</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Captive portal</td>
</tr>
<tr>
<td>cdp</td>
<td>Cisco Discovery Protocol</td>
</tr>
<tr>
<td>cluster</td>
<td>Cluster configuration</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enable persistence of configuration across reloads (startup config file)</td>
</tr>
<tr>
<td>controller</td>
<td>WLAN controller configuration</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Critical Resource</td>
</tr>
<tr>
<td>crypto</td>
<td>Encryption related commands</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Device firmware upgrade</td>
</tr>
<tr>
<td>dot1x</td>
<td>802.1X</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configure IP DSCP to 802.1p priority mapping for untagged frames</td>
</tr>
<tr>
<td>email-notification</td>
<td>Email notification configuration</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Check the firmware versions of devices before interoperating</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Environmental Sensors Configuration</td>
</tr>
<tr>
<td>events</td>
<td>System event messages</td>
</tr>
<tr>
<td>export</td>
<td>Export a file</td>
</tr>
<tr>
<td>floor</td>
<td>Set the floor within a area where the system is located</td>
</tr>
<tr>
<td>gre</td>
<td>GRE protocol</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Specify HTTP-Analysis configuration</td>
</tr>
<tr>
<td>interface</td>
<td>Select an interface to configure</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>L2tpv3 protocol</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>L3e lite Table</td>
</tr>
<tr>
<td>led</td>
<td>Turn LEDs on/off on the device</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Enable device firmware to auto downgrade when other legacy devices are detected</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto upgrade of legacy devices</td>
</tr>
<tr>
<td>lldp</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configure load balancing parameter</td>
</tr>
<tr>
<td>logging</td>
<td>Modify message logging facilities</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>MAC Address Table</td>
</tr>
<tr>
<td>mac-auth</td>
<td>802.1X</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Memory profile to be used on the device</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configure meshpoint device parameters</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configure meshpoint monitoring interval</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Check controller connectivity after configuration is received</td>
</tr>
<tr>
<td>mint</td>
<td>MiNT protocol</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Check controller connectivity after configuration is received</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configure neighbor inactivity timeout</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configure neighbor information exchange interval</td>
</tr>
<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 A.B.C.D</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>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>
</tbody>
</table>
reevaluate-everytime Set the flag to reevaluate autoprosonting policy every time
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
tunnel-controller Tunnel Controller group this controller belongs to
use Set setting to use
vrrp VRRP configuration
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
driver 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-test)#

**NOTE:** For more information on profiles and how to configure profiles, see *Chapter 7, PROFILES.*

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes a profile and its associated configurations</td>
</tr>
</tbody>
</table>
4.1.51 radio-qos-policy

Global Configuration Commands

Configures a radio quality-of-service (QoS) policy

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

Parameters

- `radio-qos-policy <RADIO-QOS-POLICY-NAME>`

Examples

```
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

```
rfs7000-37FABE(config-radio-qos-test)#
```

**NOTE:** For more information on radio qos policy, see Chapter 18, RADIO-QOS-POLICY.

Related Commands

- `no` Removes an existing Radio QoS policy
4.1.52 radius-group

Global Configuration Commands

Configures RADIUS user group parameters

Supported in the following platforms:
- Access Points — AP300, 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, 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)#

NOTE: For more information on RADIUS user group commands, see Chapter 17, RADIUS-POLICY.

Related Commands
- no: Removes an existing RADIUS group
4.1.53 `radius-server-policy`

**Global Configuration Commands**

Creates an onboard device RADIUS policy

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`radius-server-policy <RADIUS-SERVER-POLICY-NAME>`

**Parameters**

- `radius-server-policy <RADIUS-SERVER-POLICY-NAME>`

**Examples**

```
rfs7000-37FABE(config)#radius-server-policy testpolicy
rfs7000-37FABE(config-radius-server-policy-testpolicy)#?
```

Radius Configuration commands:

- `authentication` Radius authentication
- `chase-referral` Enable chasing referrals from LDAP server
- `crl-check` Enable Certificate Revocation List (CRL) check
- `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
- `use` Set setting to use
- `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-radius-server-policy-testpolicy)#
```

**NOTE:** For more information on RADIUS server policy commands, see Chapter 17, `RADIUS-POLICY`.

**Related Commands**

- `no` Removes an existing RADIUS server policy
4.1.54 **radius-user-pool-policy**

- **Global Configuration Commands**

Configures a RADIUS user pool

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>
```

**Parameters**

- `radius-user-pool-policy <RADIUS-USER-POOL-POLICY-NAME>`

| <RADIUS-USER-POOL-POLICY-NAME> | Specify the RADIUS user pool policy name. If the policy does not exist, it is created. |

**Examples**

```
rfs7000-37FABE(config)#radius-user-pool-policy testpool
rfs7000-37FABE(config-radius-user-pool-testpool)#?
```

Radius User Pool Mode commands:

```
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)#
```

---

**NOTE:** For more information on RADIUS user group commands, see Chapter 17, *RADIUS-POLICY.*

**Related Commands**

- `no` Removes an existing RADIUS user pool
4.1.55 roaming-assist-policy

**Global Configuration Commands**

Configures a roaming-assist policy

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>

**Parameters**

- roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME

<table>
<thead>
<tr>
<th>ROAMING-ASSIST-POLICY-NAME</th>
<th>Specify the roaming-assist policy name. If the policy does not exist, it is created.</th>
</tr>
</thead>
</table>

**Examples**

rfs6000-81742D(config)roaming-assist-policy test
rfs6000-81742D(config-roaming-assist-policy-test)#?

Roaming Assist Mode commands:

- action Configure action
- detection-threshold Configure the detection threshold
- handoff-count Configure the handoff count
- handoff-threshold Configure the handoff threshold
- monitoring-interval Configure the monitoring interval
- no Negate a command or set its defaults
- sampling-interval Configure the sampling interval
- 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

rfs6000-81742D(config-roaming-assist-policy-test)#

**NOTE:** For more information on roaming-assist-policy commands, see Chapter 30, ROAMING ASSIST POLICY.

**Related Commands**

- no Removes an existing roaming-assist-policy
4.1.56 **rename**

Global Configuration Commands

Renames and existing TLO

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
rename tlo <TLO-NAME>
```

Parameters

- `rename tlo <TLO-NAME> <NEW-TLO-NAME>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rename tlo</code></td>
<td>Renames an existing TLO object</td>
</tr>
<tr>
<td><code>&lt;TLO-NAME&gt;</code></td>
<td>- <code>&lt;TLO-NAME&gt;</code> -- Specify the TLO's name. This is the TLO that is to be renamed.</td>
</tr>
<tr>
<td><code>&lt;NEW-TLO-NAME&gt;</code></td>
<td>- <code>&lt;NEW-TLO-NAME&gt;</code> -- Specify the new name for this TLO</td>
</tr>
</tbody>
</table>

Note: Enter `rename` and press **Tab** to list top level objects available for renaming.

Examples

The following example shows the top level objects available for renaming:

```
rfs4000-229D58(config)#rename
aaa_policy                         aaa_tacacs_policy
address_range_alias               aif_policy
ap300                             assoc_acl
auto_provisioning_policy          bgp_as_path_list
bgp_community_list                bgp_extcommunity_list
bgp_ip_access_list                bgp_ip_prefix_list
bonjour_gw_discovery_policy       bonjour_gw_forwarding_policy
bonjour_gw_query_forwarding_policy bridging_policy
captive_portal                    centro_policy
client_identity                   client_identity_group
cryptomers_policy                 crypto_cmp_policy
device_categorization             dhcp_server_policy
dhcpv6_server_policy              dns_whitelist
dr_route_map                       event_system_policy
firewall_policy                    global_assoc_list
host_alias                         ip_acl
ip_snmp_acl                        ipv6_acl
ipv6_radv_policy                   l2tpv3_policy
mac_acl                            management_policy
meshpoint                          meshpoint_qos
mint_policy                        mint_security_policy
nac_list                           network_alias
network_group_alias                network_service_alias
passpoint_policy                   profile
radio_qos                          radius_group
radius_server_policy               radius_user_pool
rf_domain                          rls_policy
roaming_assist_policy              role_policy
routing_policy                     runtime_license
smart_rf_policy                    string_alias
subscriber_policy                  url_filter
url_list                           vlan_alias
wips_policy                        wlan
wlan_qos                           wsm_policy
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:

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.5.6.0-006D
!
! 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"
!
mac access-list PERMIT-ARP-AND-IPv4
   permit any any type ip 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 5.5.6.0-006D
!
! 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
   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"
   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
   --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 5.5.6.0-006D
!
! 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 |
4.1.57 *rf-domain*

*Global Configuration Commands*

An RF Domain groups devices that can logically belong to one network.

Table 4.16 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 4-175</td>
</tr>
<tr>
<td>rf-domain-mode commands</td>
<td>Invokes RF Domain configuration mode commands</td>
<td>page 4-177</td>
</tr>
</tbody>
</table>
4.1.57.1 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 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 in 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 — AP300, 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, NX9000, NX9500, NX9510
Syntax

rf-domain {<RF-DOMAIN-NAME>|containing <DOMAIN-NAME>}

Parameters

- rf-domain {<RF-DOMAIN-NAME>|containing <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>&lt;RF-DOMAIN-NAME&gt;</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>containing</th>
<th>Optional. Identifies an existing RF Domain that contains a specified sub-string in the domain name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DOMAIN-NAME&gt;</td>
<td>- Specify a sub-string of the RF Domain name.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config)#rf-domain rfs7000
rfs7000-37FABE(config)#rf-domain-containing rfs7000)

RF Domain Mode commands:

- alias
- channel-list
- contact
- control-vlan
- controller-managed
- country-code
- layout
- location
- mac-name
- no
- override-smartrf
- override-wlan
- sensor-server
- stats
- timezone
- tree-node
- use
- clrscr
- commit
- do
- end
- exit
- help
- revert
- service
- show
- write

rfs7000-37FABE(config-rf-domain-rfs7000)#
4.1.57.2 rf-domain-mode commands

rf-domain

This section describes the default commands under RF Domain.

Table 4.17 summarises RF Domain configuration commands.

Table 4.17 RF-Domain-Mode 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 4-178</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures the channel list advertised by radios</td>
<td>page 4-183</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 4-184</td>
</tr>
<tr>
<td>control-vlan</td>
<td>Configures VLAN for traffic control on a RF Domain</td>
<td>page 4-185</td>
</tr>
<tr>
<td>controller-managed</td>
<td>Configures the adopting controller or service platform as this RF Domain’s manager</td>
<td>page 4-186</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures the country of operation</td>
<td>page 4-187</td>
</tr>
<tr>
<td>layout</td>
<td>Configures layout information</td>
<td>page 4-188</td>
</tr>
<tr>
<td>location</td>
<td>Configures the physical location of a RF Domain</td>
<td>page 4-190</td>
</tr>
<tr>
<td>mac-name</td>
<td>Maps MAC addresses to names</td>
<td>page 4-191</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts configured settings to their default</td>
<td>page 4-192</td>
</tr>
<tr>
<td>override-smart-rf</td>
<td>Configures RF Domain level overrides for Smart RF</td>
<td>page 4-194</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configures RF Domain level overrides for a WLAN</td>
<td>page 4-195</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server on this RF Domain</td>
<td>page 4-196</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 4-198</td>
</tr>
<tr>
<td>timezone</td>
<td>Configures a RF Domain’s geographic time zone</td>
<td>page 4-199</td>
</tr>
<tr>
<td>tree-node</td>
<td>Configures the hierarchial (tree-node) structure under which this RF Domain appears</td>
<td>page 4-200</td>
</tr>
<tr>
<td>use</td>
<td>Enables the use of a specified Smart RF and/or WIPS policy</td>
<td>page 4-202</td>
</tr>
</tbody>
</table>
4.1.57.2.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

alias [address-range|host|network|network-group|network-service|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>

Parameter

- alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

  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.

  - <ADDRESS-RANGE-ALIAS-NAME> — Specify the address range alias name.

  **Note:** Alias name should begin with `$`.

- <STARTING-IP> to <ENDING-IP>

  Associates a range of IP addresses with this address range alias

  - <STARTING-IP> — Specify the first IP address in the range.
  - to <ENDING-IP> — Specify the last IP address in the range.

  **Note:** If using an existing address-range alias, you can apply overrides to the alias at the RF Domain level.
### GLOBAL CONFIGURATION COMMANDS

#### 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>&lt;HOST-ALIAS-NAME&gt;</td>
<td>Specify the host alias name. <strong>Note:</strong> Alias name should begin with <code>$</code>.</td>
</tr>
<tr>
<td>&lt;HOST-IP&gt;</td>
<td>Associates the network host’s IP address with this host alias. <strong>Note:</strong> If using an existing host alias, you can apply overrides to the alias at the RF Domain level.</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>&lt;NETWORK-ALIAS-NAME&gt;</td>
<td>Specify the network alias name. <strong>Note:</strong> Alias name should begin with <code>$</code>.</td>
</tr>
<tr>
<td>&lt;NETWORK-ADDRESS/MASK&gt;</td>
<td>Associates a single network with this network alias. <strong>Note:</strong> If using an existing network alias, you can apply overrides to the alias at the RF Domain level.</td>
</tr>
</tbody>
</table>

#### alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</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>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</td>
<td>Specify the network-group alias name. <strong>Note:</strong> Alias name should begin with <code>$</code>.</td>
</tr>
<tr>
<td>address-range</td>
<td>Associates a range of IP addresses with this network-group alias. <strong>Note:</strong> After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses. <strong>Note:</strong> If using an existing network-group alias, you can apply overrides to the alias at the RF Domain level.</td>
</tr>
<tr>
<td>{&lt;STARTING-IP&gt; to &lt;ENDING-IP&gt;}</td>
<td>Specify the first IP address in the range.</td>
</tr>
<tr>
<td>to {&lt;STARTING-IP&gt; to &lt;ENDING-IP&gt;}</td>
<td>to &lt;ENDING-IP&gt; – Specify the last IP address in the range.</td>
</tr>
<tr>
<td>host &lt;HOST-IP&gt; {&lt;HOST-IP&gt;}</td>
<td>Associates a single or multiple hosts with this network-group alias. <strong>Note:</strong> Specifies more than one host. A maximum of eight (8) hosts can be configured.</td>
</tr>
<tr>
<td>network &lt;NETWORK-ADDRESS/MASK&gt; {&lt;NETWORK-ADDRESS/MASK&gt;}</td>
<td>Associates a single or multiple networks with this network-group alias. <strong>Note:</strong> Specifies more than one network. A maximum of eight (8) networks can be configured.</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.
| | • 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|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 News group (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.
| Contd..
GLOBAL CONFIGURATION COMMANDS

- **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 `$DOMAIN test.company.com` In this example, the string alias name is: `$DOMAIN` and the string value it is mapped to is: `test.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.
  - `<1-4094>` – Specify the VLAN ID from 1 - 4094.

  **Note:** Alias name should begin with `$`.

  **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 RF Domain level.

**Examples**

```
rfs4000-229D58 (config)# show context

! Configuration of RFS4000 version 5.5.6.0-006D
!
! 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 $TestVLAN Alias 1
rfs4000-229D58 (config) #

In the following examples the global aliases '$kerberos' and '$TestVLAN Alias' 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 $TestVLAN Alias 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 vlan $TestVLAN Alias 10
rfs4000-229D58 (config-rf-domain-test) #

nx9500-6C8809 (config-rf-domain-test) # alias string $test company.com

nx9500-6C8809 (config-rf-domain-test) # show context
rf-domain test
  no country-code
  alias string $test company.com
nx9500-6C8809 (config-rf-domain-test) #

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 $TestVLAN Alias 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>no</td>
<td>Removes a network, network-group, network-service, VLAN, or string alias from this RF Domain</td>
</tr>
</tbody>
</table>
4.1.57.2.2 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 — AP300, 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, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Enables a dynamic update of a channel list</td>
</tr>
</tbody>
</table>

- channel-list [2.4GHz|5GHz] <CHANNEL-LIST>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz &lt;CHANNEL-LIST&gt;</td>
<td>Configures the channel list advertised by radios operating in the 2.4 GHz mode</td>
</tr>
<tr>
<td>5GHz &lt;CHANNEL-LIST&gt;</td>
<td>Configures the channel list advertised by radios operating in the 5.0 GHz mode</td>
</tr>
</tbody>
</table>

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.
4.1.57.2.3 **contact**

<table>
<thead>
<tr>
<th>rf-domain-mode commands</th>
</tr>
</thead>
</table>

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 — AP300, 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, 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
4.1.57.2.4 control-vlan

* rf-domain-mode commands

Configures the VLAN designated for traffic control in this RF Domain

Supported in the following platforms:

- Access Points — AP300, 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, 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
4.1.57.2.5 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 — AP300, 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, NX5524, NX7500, 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
  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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the adopting controller or service platform as this RF Domain’s manager</td>
</tr>
</tbody>
</table>
4.1.57.2.6 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 — AP300, 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, 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
### 4.1.57.2.7 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
layout [area|floor|map-location]
layout area <AREA-NAME> {floor|map-location}
layout floor <FLOOR-NAME>{1-4094|area|map-location}
layout map-location <URL> units [feet|meters] {area <AREA-NAME>|floor <FLOOR-NAME>}
```

**Parameters**

- **layout area <AREA-NAME> {floor|map-location}**
  - **area <AREA-NAME>** Configures the RF Domain’s area name
    - `<AREA-NAME>` – Specify the area name.
    - **Note:** After configuring the RF Domain’s area of functioning, optionally specify the floor name (and number), and/or the map location.

- **layout floor <FLOOR-NAME>{1-4094|area|map-location}**
  - **floor <FLOOR-NAME>** Configures the RF Domain’s floor name
    - `<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 and/or the map location.

- **layout map-location <URL> units [feet|meters] {area <AREA-NAME>|floor <FLOOR-NAME>}**
  - **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.
    - **Note:** units [feet|meters] – Configures the map units in terms of feet or meters

<table>
<thead>
<tr>
<th><strong>layout</strong></th>
<th><strong>Description</strong></th>
<th><strong>Parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>area &lt;AREA-NAME&gt;</td>
<td>Configures the RF Domain’s layout in terms of area, floor, and location on a map</td>
<td></td>
</tr>
<tr>
<td>floor &lt;FLOOR-NAME&gt;</td>
<td>Configures the RF Domain’s floor name</td>
<td><code>&lt;FLOOR-NAME&gt;</code> – Specify the floor name.\n</td>
</tr>
<tr>
<td>map-location &lt;URL&gt; units [feet</td>
<td>meters]</td>
<td>Configures the location of the RF Domain on the map</td>
</tr>
<tr>
<td>area &lt;AREA-NAME&gt;</td>
<td>Optional. Configures the RF Domain’s area name. Specify area name.</td>
<td><strong>Note:</strong> After configuring the RF Domain’s area name, optionally specify the floor name and number</td>
</tr>
<tr>
<td>floor &lt;FLOOR-NAME&gt;</td>
<td>Optional. Configures the RF Domain’s floor name. Specify floor name.</td>
<td><strong>Note:</strong> After configuring the floor name (and number) for this RF Domain, optionally specify the area name.</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-rf-domain-default)#layout map-location www.firstfloor.com units meters area Ecospace floor Floor5

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 Floor5 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>no</td>
<td>Removes the RF Domain layout details</td>
</tr>
</tbody>
</table>
4.1.57.2.8 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 common set of device configurations are deployed and managed by a RF Domain policy.

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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
country-code us
control-vlan 1

Related Commands

- no

Removes the RF Domain location
4.1.57.2.9 mac-name

**rf-domain-mode commands**

Configures a relevant name for each MAC address

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mac-name <MAC> <NAME>
```

**Parameters**

- **mac-name** `<MAC>` `<NAME>`

<table>
<thead>
<tr>
<th>mac-name</th>
<th>Configures a relevant name for each MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAC&gt;</code> <code>&lt;NAME&gt;</code></td>
<td>Specifies the MAC address</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;NAME&gt;</code> – Specify a friendly name for this MAC address to use in events and statistics.</td>
</tr>
</tbody>
</table>

**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 |
4.1.57.2.10 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 — AP300, 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, 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 alias Removes aliases associated with this RF Domain
- no channel-list Removes the channel list for the 2.4 GHz and 5.0 GHz bands. Also disables dynamic update of a channel list.
- no contact Removes configured contact details
- no control-vlan Removes the VLAN configured for controlling traffic
- no controller-managed Removes the adopting controller (access point, wireless controller, or service platform) as this RF Domain’s manager
- no country-code Removes the country of operation configured
- no layout Removes RF Domain layout details
- no location Removes RF Domain location details
- no mac-name Removes the MAC address to name mapping
- no override-smartrf Resets override Smart RF settings to default
- no override-wlan Resets override WLAN settings to default
- no sensor-server Disables AirDefense sensor server details
- no stats Resets RF Domain stats settings
- no timezone Removes RF Domain’s time zone
- no tree-node Removes the configured hierarchial (tree-node) structure under which this RF Domain appears
- no use Resets RF Domain profile settings
Examples
The following example shows the default RF Domain settings before the ‘no’ commands are executed:

```
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)#
```

```
rfs7000-37FABE(config-rf-domain-default)#no channel-list 2.4GHz 1-10
rfs7000-37FABE(config-rf-domain-default)#no mac-name 11-22-33-44-55-66
rfs7000-37FABE(config-rf-domain-default)#no location
rfs7000-37FABE(config-rf-domain-default)#no control-vlan
```

The following example shows the default RF Domain settings after the ‘no’ commands are executed:

```
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
    contact Bob+14082778691
    country-code us
    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>alias</td>
<td>Configures network, VLAN, and service aliases at the RF Domain level</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures the channel list advertised by radios, and enables dynamic update of channel lists</td>
</tr>
<tr>
<td>contact</td>
<td>Configures details of the person to contact (or the administrator) in case of any problems or issues impacting the RF Domain</td>
</tr>
<tr>
<td>control-vlan</td>
<td>Configures a VLAN for traffic control</td>
</tr>
<tr>
<td>controller-managed</td>
<td>Configures the adopting controller or service platform as this RF Domain’s manager</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures a RF Domain’s country of operation</td>
</tr>
<tr>
<td>layout</td>
<td>Configures a RF Domain’s layout maps</td>
</tr>
<tr>
<td>location</td>
<td>Configures a RF Domain’s deployment location</td>
</tr>
<tr>
<td>mac-name</td>
<td>Configures a relevant name for each MAC address</td>
</tr>
<tr>
<td>override-smart-rf</td>
<td>Configures RF Domain level overrides for Smart RF</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configures RF Domain level overrides for WLAN</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server</td>
</tr>
<tr>
<td>stats</td>
<td>Configures RF Domain stats settings</td>
</tr>
<tr>
<td>timezone</td>
<td>Configures a RF Domain’s geographic time zone</td>
</tr>
<tr>
<td>tree-node</td>
<td>Configures the hierarchial (tree-node) structure under which this RF Domain appears</td>
</tr>
<tr>
<td>use</td>
<td>Enables the use of a Smart RF and/or WIPS policy</td>
</tr>
</tbody>
</table>
4.1.57.2.11 override-smart-rf

Enable dynamic channel switching for Smart RF radios

Supported in the following platforms:
- Access Points — AP300, 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, 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>override-smartrf</td>
<td>Enables dynamic channel switching for Smart RF radios</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures a list of channels for 2.4 GHz and 5.0 GHz Smart RF radios</td>
</tr>
<tr>
<td>2.4GHz &lt;CHANNEL-LIST&gt;</td>
<td>Selects the 2.4 GHz Smart RF radio channels</td>
</tr>
<tr>
<td>5GHz &lt;CHANNEL-LIST&gt;</td>
<td>Selects the 5.0 GHz Smart RF radio channels</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
contact Bob+14082778691
country-code us
override-smart-rf channel-list 2.4GHz 1,2,3
layout area Ecospaces floor Floor5 map-location www.firstfloor.com units meters
rfs7000-37FABE(config-rf-domain-default)#

Related Commands
- no Resets the override Smart RF settings its default
4.1.57.2.12 override-wlan

rf-domain-mode commands

Configures RF Domain level overrides for a WLAN

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

overrides-wlan <WLAN> [ssid|vlan-pool|wpa-wpa2-psk]

overrides-wlan <WLAN> [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>} | wpa-wpa2-psk <PASSPHRASE>]

Parameters

- overrides-wlan <WLAN> [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>} | wpa-wpa2-psk <PASSPHRASE>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WLAN&gt;</td>
<td>Configures the WLAN name. The name should not exceed 32 characters and should represent the WLAN coverage area. After creating the WLAN, configure its override parameters.</td>
</tr>
<tr>
<td>ssid &lt;SSID&gt;</td>
<td>Configures a override SSID associated with this WLAN. The SSID should not exceed 32 characters.</td>
</tr>
<tr>
<td>vlan-pool &lt;1-4094&gt; {limit &lt;0-8192&gt;}</td>
<td>Configures the override VLANs available to this WLAN.</td>
</tr>
<tr>
<td>wpa-wpa2-psk &lt;PASSPHRASE&gt;</td>
<td>Configures the WPA-WPA2 pre-shared key or passphrase for this WLAN.</td>
</tr>
</tbody>
</table>

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

no | Resets the override WLAN settings its default |
4.1.57.2.13 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}
```

Parameters

- **Sensor-server <1-3>**
  - Configures an AirDefense sensor server parameters
  - `<1-3>` – Select the server ID from 1 - 3. The server with the lowest defined ID is reached first. The default is 1.

- **ip <IP>**
  - Configures the (non DNS) IP address of the sensor server
  - `<IP>` – Specify the IP address of the sensor server.

- **port [443|8443|<1-65535>]**
  - Optional. Configures the sensor server port. The options are:
    - `443` – Configures port 443, the default port used by the AirDefense server
    - `8843` – Configures port 883, the default port used by advanced WIPS
    - `<1-65535>` – Allows you to select a WIPS/AirDefense sensor server port from 1 - 65535
Examples

```
rfs7000-37FABE(config-rf-domain-default)#sensor-server 2 ip 172.16.10.3 port 443
rfs7000-37FABE(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
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>Disables an AirDefense sensor server parameters</td>
</tr>
</tbody>
</table>
4.1.57.2.14 stats

rf-domain-mode commands

Configures stats settings that define how RF Domain statistics are updated

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

stats [open-window|update-interval]
stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
stats update-interval [<5-300]|auto

Parameters

- stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
- stats update-interval [<5-300]|auto

<table>
<thead>
<tr>
<th>stats</th>
<th>Configures stats related settings on this RF Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>open-window &lt;1-2&gt;</td>
<td>Opens a stats window to get trending data</td>
</tr>
<tr>
<td>sample-interval &lt;5-86640&gt;</td>
<td>Optional. Configures the interval at which the wireless controller captures statistics supporting this RF Domain</td>
</tr>
<tr>
<td>size &lt;3-100&gt;</td>
<td>Optional. After specifying the interval time, specify the number of samples used to define RF Domain statistics.</td>
</tr>
</tbody>
</table>

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
  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
4.1.57.2.15 timezone

rf-domain-mode commands

Configures the RF Domain’s geographic time zone. Configuring the time zone is essential for RF Domains deployed across different geographical locations.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

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

Related Commands

no Removes a RF Domain’s time zone
4.157.2.16 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 — AP300, 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, 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}

| tre-node   | Configures the hierarchical tree structure defining the RF Domain’s location. The tree node hierarchy can be configured in any order, but will always appear as: country > region > city > campus. Further, a higher node, such as country, cannot be defined under a lower node, such as region. An RF Domain can be placed under any one of the tree nodes. But, an RF Domain at the country level may have all four nodes defined. Where as, an RF Domain restricted to a campus, cannot have the country, city, and region nodes.
|            | **Note:** At least one of these four nodes must be defined. This feature is disabled by default.

- campus Configures the campus name for this RF Domain
- city Configures the city for this RF Domain
- country Configures the country for this RF Domain
- region Configures the region for this RF Domain

Usage Guidelines
The following points need to be taken into consideration when creating the tree-node structure:

- 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 mapped 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.
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

| no       | Removes the RF Domain's tree-node configuration |
4.1.57.2.17 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 lock down, or port suppression

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
use [smart-rf-policy|wips-policy]
use [smart-rf-policy <SMART-RF-POLICY-NAME>|wips-policy <WIPS-POLICY-NAME>]
```

Parameters

- use [smart-rf-policy <SMART-RF-POLICY-NAME>|wips-policy <WIPS-POLICY-NAME>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>Uses a Smart RF policy with this RF Domain</td>
</tr>
<tr>
<td>smart-rf-policy</td>
<td>Specifies a Smart RF policy</td>
</tr>
<tr>
<td>&lt;SMART-RF-POLICY-NAME&gt;</td>
<td>- Specify the Smart RF policy name. For more information on configuring smart RF policy, see SMART-RF-POLICY.</td>
</tr>
<tr>
<td>wips-policy</td>
<td>Specifies a WIPS policy</td>
</tr>
<tr>
<td>&lt;WIPS-POLICY-NAME&gt;</td>
<td>- Specify the WIPS policy name. For more information on configuring WIPS policy, see WIPS-POLICY.</td>
</tr>
</tbody>
</table>

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><code>no</code></td>
<td>Resets profiles used with this RF Domain</td>
</tr>
<tr>
<td><code>sensor-server</code></td>
<td>Configures an AirDefense sensor server on this RF Domain</td>
</tr>
<tr>
<td><code>wips-policy</code></td>
<td>Configures a WIPS policy</td>
</tr>
<tr>
<td><code>smart-rf-policy</code></td>
<td>Configures a Smart RF policy</td>
</tr>
</tbody>
</table>
## 4.1.58 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

### Syntax

```
rfs4000 <DEVICE-RFS4000-MAC>
```

### Parameters

- `rfs4000 <DEVICE-RFS4000-MAC>`

<table>
<thead>
<tr>
<th>&lt;DEVICE-RFS4000-MAC&gt;</th>
<th>Specify the RFS4000’s MAC address.</th>
</tr>
</thead>
</table>

### 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 |
4.1.59  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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
rfs6000 <DEVICE-RFS6000-MAC>
```

Parameters

- `rfs6000 <DEVICE-RFS6000-MAC>`

<table>
<thead>
<tr>
<th>&lt;DEVICE-RFS6000-MAC&gt;</th>
<th>Specify the RFS6000's MAC address.</th>
</tr>
</thead>
</table>

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
4.1.60 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, NX6500, NX6524, NX7500, 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 |
4.1.61 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, NX6500, NX6524, NX7500, 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**

- `<DEVICE-NX45XX-MAC>`

**Examples**

```
x9500-6C8809(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
4.1.62  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, NX6500, NX6524, NX7500, 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
4.1.63 `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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
nx75xx <DEVICE-NX75XX-MAC>
```

**Parameters**

- `nx75xx <DEVICE-NX75XX-MAC>`

<table>
<thead>
<tr>
<th><code>&lt;DEVICE-NX75XX-MAC&gt;</code></th>
<th>Specifies the MAC address of a NX75XX series service platform.</th>
</tr>
</thead>
</table>

**Examples**

```
nx9500-6C8809(config)#nx75xx 00-23-45-FA-06-38
nx9500-6C8809(config-device-00-23-45-FA-06-38)#
```

**Related Commands**

| `no` | Removes a NX75XX series service platform from the network |
4.1.64 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, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

nx9000 <DEVICE-NX9000-MAC>

Parameters

- nx9000 <DEVICE-NX9000-MAC>

<DEVICE-NX9000-MAC> Specifies the MAC address of a NX9000 series service platform.

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
4.1.65 role-policy

Configures a role-based firewall policy

Supported in the following platforms:
- Access Points — AP300, 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, 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-server        Add a ldap server
  - ldap-service       Enable ldap attributes in role definition
  - 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 19, ROLE-POLICY.

Related Commands
- no            Removes an existing role policy
4.1.66 routing-policy

Global Configuration Commands

Configures a routing policy

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

role-policy <ROUTING-POLICY-NAME>

Parameters

- role-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
disable End current mode and change to EXEC mode
default End current mode and down to previous mode
desc Description of the interactive help system
revert Revert changes
start 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 25, ROUTING-POLICY.

Related Commands

- no Removes an existing routing policy
4.1.67 self

Display the device’s configuration context

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
self
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config)#self
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```
4.1.68 smart-rf-policy

**Global Configuration Commands**

Configures a Smart RF policy

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

smart-rf-policy <SMART-RF-POLICY-NAME>

**Parameters**

- `smart-rf-policy <SMART-RF-POLICY-NAME>`

**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
- `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 20, SMART-RF-POLICY.

**Related Commands**

- `no` Removes an existing Smart RF policy
4.1.69 **wips-policy**

> **Global Configuration Commands**

Configures a WIPS policy

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wips-policy <WIPS-POLICY-NAME>
```

**Parameters**

- **wips-policy <WIPS-POLICY-NAME>**

| <WIPS-POLICY-NAME> | Specify the WIPS policy name. If the policy does not exist, it is created. |

**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** 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-wips-policy-test)#
```

**NOTE:** For more information on WIPS policy commands, see *Chapter 21, WIPS-POLICY.*

**Related Commands**

- **no** Removes an existing WIPS policy
4.1.70 wlan

- **Global Configuration Commands**

Configures a *Wireless Local Area Network* (WLAN)

Table 4.18 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 4-217</td>
</tr>
<tr>
<td>wlan-mode</td>
<td>Summarizes WLAN configuration mode commands</td>
<td>page 4-220</td>
</tr>
</tbody>
</table>

Table 4.18 WLAN-Policy Config Commands
4.1.70.1 wlan

`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 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.

RFS4000 and RFS6000 controllers and NX4500 and NX6500 service platforms support a maximum of 32 WLANs. The RFS7000 model wireless controller supports up to 256 WLANs. A NX9000 series service platform supports up to 1000 WLANs. An access point supports a maximum of 16 WLANs.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

**Parameters**

- wlan `{<WLAN-NAME>|containing <WLAN-NAME>}`

<table>
<thead>
<tr>
<th>wlan <code>&lt;WLAN-NAME&gt;</code></th>
<th>Configures a new WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;WLAN-NAME&gt;</code> — Optional. Specify the WLAN name.</td>
<td></td>
</tr>
<tr>
<td>The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing etc.). The name cannot exceed 32 characters.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>containing <code>&lt;WLAN-NAME&gt;</code></th>
<th>Optional. Configures an existing WLAN's settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;WLAN-NAME&gt;</code> — Specify a sub-string in the WLAN name. Use this parameter to filter a WLAN.</td>
<td></td>
</tr>
<tr>
<td>This option allows you to select and enter the configuration mode of one or more WLANs.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#wlan 1
rfs7000-37FABE(config-wlan-1)#
```

```
rfs7000-37FABE(config)#wlan containing wlan1
rfs7000-37FABE(config-wlan-{'containing': 'wlan1'})#```
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>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>kerberos</td>
<td>Configure kerberos authentication parameters</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>Configure mac-authentication related parameters</td>
</tr>
<tr>
<td>mac-registration</td>
<td>Enable dynamic MAC registration of user</td>
</tr>
<tr>
<td>wing-extensions</td>
<td>Enable support for WiNG-Specific extensions to 802.11</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</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>radio-resource-measurement</td>
<td>Configure support for 802.11k Radio Resource Measurement</td>
</tr>
<tr>
<td>radius</td>
<td>Configure RADIUS related parameters</td>
</tr>
<tr>
<td>relay-agent</td>
<td>Configure dhcp relay agent info</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown this wlan</td>
</tr>
<tr>
<td>ssid</td>
<td>Configure the Service Set Identifier for this WLAN</td>
</tr>
<tr>
<td>time-based-access</td>
<td>Configure client access based on time</td>
</tr>
</tbody>
</table>
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
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)#
### 4.1.70.2 wlan-mode commands

**wlan**

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>
```

Table 4.19 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 4-222</td>
</tr>
<tr>
<td>acl</td>
<td>Defines the actions based on an ACL rule configuration</td>
<td>page 4-224</td>
</tr>
<tr>
<td>answer-broadcast-probes</td>
<td>Allows a WLAN to respond to probes for broadcast ESS</td>
<td>page 4-226</td>
</tr>
<tr>
<td>association-list</td>
<td>Attaches an existing global association list to a WLAN</td>
<td>page 4-227</td>
</tr>
<tr>
<td>authentication-type</td>
<td>Sets a WLAN’s authentication type</td>
<td>page 4-228</td>
</tr>
<tr>
<td>bridging-mode</td>
<td>Configures how packets to/from this WLAN are bridged</td>
<td>page 4-230</td>
</tr>
<tr>
<td>broadcast-dhcp</td>
<td>Configures broadcast DHCP packet handling</td>
<td>page 4-231</td>
</tr>
<tr>
<td>broadcast-ssid</td>
<td>Advertises a WLAN’s SSID in beacons</td>
<td>page 4-232</td>
</tr>
<tr>
<td>captive-portal-enforcement</td>
<td>Configures a WLAN’s captive portal enforcement</td>
<td>page 4-233</td>
</tr>
<tr>
<td>client-access</td>
<td>Enables WLAN client access (normal data operations)</td>
<td>page 4-234</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 4-235</td>
</tr>
<tr>
<td>client-load-balancing</td>
<td>Enables load balancing of WLAN clients</td>
<td>page 4-236</td>
</tr>
<tr>
<td>controller-assisted-mobility</td>
<td>Enables controller assisted mobility to determine wireless clients’ VLAN assignment</td>
<td>page 4-238</td>
</tr>
<tr>
<td>data-rates</td>
<td>Specifies the 802.11 rates supported on the WLAN</td>
<td>page 4-239</td>
</tr>
<tr>
<td>description</td>
<td>Sets a WLAN’s description</td>
<td>page 4-242</td>
</tr>
<tr>
<td>downstream-group-addressed-forwarding</td>
<td>Enables forwarding of downstream packets addressed to a group</td>
<td>page 4-243</td>
</tr>
<tr>
<td>dynamic-vlan-assignment</td>
<td>Configures dynamic VLAN assignment on this WLAN</td>
<td>page 4-244</td>
</tr>
<tr>
<td>eap-types</td>
<td>Configures client access based on eap-type used for authentication</td>
<td>page 4-245</td>
</tr>
<tr>
<td>encryption-type</td>
<td>Sets a WLAN’s encryption type</td>
<td>page 4-246</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>enforce-dhcp</td>
<td>Drops packets from clients with a static IP address</td>
<td>page 4-247</td>
</tr>
<tr>
<td>fast-bss-transition</td>
<td>Configures support for 802.11r fast BSS transition on a WLAN</td>
<td>page 4-248</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enables HTTP URL analysis on the WLAN</td>
<td>page 4-249</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP settings</td>
<td>page 4-250</td>
</tr>
<tr>
<td>kerberos</td>
<td>Configures Kerberos authentication parameters</td>
<td>page 4-251</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>Configures MAC authentication parameters</td>
<td>page 4-253</td>
</tr>
<tr>
<td>mac-registration</td>
<td>Enables dynamic MAC registration of user</td>
<td>page 4-254</td>
</tr>
<tr>
<td>wing-extensions</td>
<td>Enables support for WiNG specific extensions to 802.11</td>
<td>page 4-256</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 4-257</td>
</tr>
<tr>
<td>proxy-arp-mode</td>
<td>Enables the proxy ARP mode for ARP requests</td>
<td>page 4-260</td>
</tr>
<tr>
<td>radio-resource-</td>
<td>Enables support for 802.11k radio resource measurement</td>
<td>page 4-261</td>
</tr>
<tr>
<td>measurement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radius</td>
<td>Configures RADIUS parameters</td>
<td>page 4-262</td>
</tr>
<tr>
<td>relay-agent</td>
<td>Enables support for DHCP relay agent information (option 82) feature on this</td>
<td>page 4-263</td>
</tr>
<tr>
<td></td>
<td>WLAN</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>Closes a WLAN</td>
<td>page 4-264</td>
</tr>
<tr>
<td>ssid</td>
<td>Configures a WLAN’s SSID</td>
<td>page 4-265</td>
</tr>
<tr>
<td>time-based-access</td>
<td>Configures time-based client access</td>
<td>page 4-266</td>
</tr>
<tr>
<td>use</td>
<td>Defines WLAN mode configuration settings</td>
<td>page 4-267</td>
</tr>
<tr>
<td>vlan</td>
<td>Sets VLAN assignment for a WLAN</td>
<td>page 4-270</td>
</tr>
<tr>
<td>vlan-pool-member</td>
<td>Adds a member VLAN to the pool of VLANs for a WLAN</td>
<td>page 4-271</td>
</tr>
<tr>
<td>wep128</td>
<td>Configures WEP128 parameters</td>
<td>page 4-272</td>
</tr>
<tr>
<td>wep64</td>
<td>Configures WEP64 parameters</td>
<td>page 4-274</td>
</tr>
<tr>
<td>wireless-client</td>
<td>Configures the transmit power for wireless clients transmission</td>
<td>page 4-276</td>
</tr>
<tr>
<td>wpa-wpa2</td>
<td>Modifies TKIP and CCMP (WPA/WPA2) related parameters</td>
<td>page 4-278</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands applicable in the WLAN configuration mode</td>
<td>page 4-281</td>
</tr>
</tbody>
</table>
4.1.70.2.1 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

accounting [radius|syslog|wait-client-ip]

accounting [radius]

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]}

  accounting syslog Enables support for WLAN syslog accounting messages in standard syslog format (RFC 3164). This option is disabled by default.
### GLOBAL CONFIGURATION COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>host</strong> &lt;IP/HOSTNAME&gt;</td>
<td>Configures a syslog destination hostname or IP address for accounting records&lt;br&gt;  • &lt;IP/HOSTNAME&gt; – Specify the IP address or name of the destination host.</td>
</tr>
<tr>
<td><strong>port</strong> &lt;1-65535&gt;</td>
<td>Optional. Configures the syslog server's UDP port (this port is used to connect to the server)&lt;br&gt;  • &lt;1-65535&gt; – Specify the port from 1 - 65535. Default port is 514.</td>
</tr>
<tr>
<td><strong>proxy-mode</strong> [none</td>
<td>through-controller</td>
</tr>
</tbody>
</table>

- **accounting syslog**<br>  Enables support for WLAN syslog accounting messages |
- **mac-address-format** | Configures the MAC address format used in syslog messages |
- **middle-hyphen** | Configures the MAC address format with middle hyphen (AABBCC-DDEEFF) |
- **no-delim** | Configures the MAC address format without delimiters (AABBCCDDEEFF) |
- **pair-colon** | Configures the MAC address format with pair-colon delimiters (AA:BB:CC:DD:EE:FF) |
- **pair-hyphen** | Configures the MAC address format with pair-hyphen delimiters (AA-BB-CC-DD-EE-FF). This is the default setting. |
- **quad-dot** | Configures the MAC address format with quad-dot delimiters (AABB.CCDD.EEFF) |
- **case** [lower|upper] | The following keywords are common to all:<br>  • case – Specifies MAC address case (upper or lower)<br>  • lower – Specifies MAC address is filled in lower case (for example, aa-bb-cc-dd-ee-ff)<br>  • upper – Specifies MAC address is filled in upper case (for example, AA-BB-CC-DD-EE-FF) |

**Examples**

```
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)#
```
4.1.70.2.2 acl

Defines the actions taken based on an ACL rule configuration.

Use the command `acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist|disassociate}` 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 Wireless Firewall.

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
 acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist|disassociate}
```

Parameters

- **acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>|disassociate}**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl exceed-rate</td>
<td>Sets the actions taken based on an ACL rule configuration (for example, drop a packet)</td>
</tr>
<tr>
<td>wireless-client-denied-traffic</td>
<td>Sets the action to deny traffic to the wireless client when the rate exceeds the specified value</td>
</tr>
<tr>
<td>&lt;0-1000000&gt;</td>
<td>&lt;0-1000000&gt; – Specify a allowed rate threshold of disallowed traffic in packets/sec.</td>
</tr>
<tr>
<td>blacklist &lt;0-86400&gt;</td>
<td>Optional. When enabled, sets the time interval to blacklist a wireless client</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)#
4.1.70.2.3 answer-broadcast-probes

wlan-mode commands

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

answer-broadcast-probes

Parameters

None

Examples

rfs7000-37FABE(config-wlan-1)#answer-broadcast-probes
rfs7000-37FABE(config-wlan-1)#
4.1.70.2.4 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`association-list global <GLOBAL-ASSO-LIST-NAME>`

**Parameters**

None

**Examples**

```
rfs4000-229D58 (config-wlan-test)#association-list global my-clients
rfs4000-229D58 (config-wlan-test)#
```

```
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)#
```
4.1.70.2.5 authentication-type

Sets the WLAN's authentication type

Supported in the following platforms:
- Access Points — AP300, 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, 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>

<table>
<thead>
<tr>
<th>eap</th>
<th>Configures EAP authentication (802.1X)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

| 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 passcode during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP. |

| kerberos             | Configures Kerberos authentication (encryption will change to WEP128 if it's not already WEP128 or Keyguard) 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). |
mac

<table>
<thead>
<tr>
<th>mac</th>
<th>Configures MAC authentication (RADIUS lookup of MAC address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP.</td>
</tr>
<tr>
<td></td>
<td>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)</td>
</tr>
<tr>
<td></td>
<td>MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date restrictions.</td>
</tr>
<tr>
<td></td>
<td>MAC authentication can only identify devices, not users.</td>
</tr>
</tbody>
</table>

| none | No authentication is used or the client uses pre-shared keys |

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)#
4.1.70.2.6 bridging-mode

<table>
<thead>
<tr>
<th>wlan-mode commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures how packets are bridged to and from a WLAN</td>
</tr>
</tbody>
</table>

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

bridging-mode [local|tunnel]

**Parameters**

- bridging-mode [local|tunnel]

<table>
<thead>
<tr>
<th>bridging-mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Bridges packets between WLAN and local ethernet ports</td>
</tr>
<tr>
<td>tunnel</td>
<td>Tunnels packets to other devices (typically a wireless controller or service platform). This is the default mode.</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)#
4.1.70.2.7 broadcast-dhcp

Configure broadcast DHCP packet parameters

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

broadcast-dhcp validate-offer

Parameters

- broadcast-dhcp validate-offer

| validate-offer       | Validates the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air |

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)#
4.1.70.2.8 broadcast-ssid

- wlan-mode commands

Advertises the WLAN SSID in beacons. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

broadcast-ssid

Parameters

None

Examples

rfs7000-37FABE(config-wlan-1)#broadcast-ssid
rfs7000-37FABE(config-wlan-1)#
4.1.70.2.9 captive-portal-enforcement

- wlan-mode commands

Configures the WLAN's captive portal enforcement

Supported in the following platforms:
- Access Points — AP300, 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, 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</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)#
```
4.1.70.2.10 client-access

- *wlan-mode commands*

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
client-access
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-wlan-1)# client-access
rfs7000-37FABE(config-wlan-1)#
```
4.1.70.2.11 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
client-client-communication

Parameters
None

Examples
rfs7000-37FABE(config-wlan-1)#client-client-communication
rfs7000-37FABE(config-wlan-1)#
4.1.70.2.12 client-load-balancing

> wlan-mode commands

Configures client load balancing on a WLAN. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
client-load-balancing
```

```
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 {allow-single-band-clients [2.4Ghz|5Ghz]}**
  - Optional. Allows single band clients to associate even during load balancing
  - 2.4GHz – Enables load balancing across 2.4 GHz channels
  - 5GHz – Enables load balancing across 5.0 GHz channels

- **band-discovery-intvl <0-10000>**
  - Optional. Configures the interval to discover a client’s band capability before connection
  - <0-10000> – Specify a value from 0 - 10000 seconds.

- **capability-ageout-time <0-10000>**
  - Optional. Configures a client’s capability ageout interval
  - <0-10000> – Specify a value from 0 - 10000 seconds.

- **max-probe-req [2.4Ghz|5Ghz] <0-10000>**
  - Optional. Configures WLAN client load balancing
  - 2.4GHz – Configures maximum client probe requests on 2.4 GHz radios
  - 5GHz – Configures maximum client probe requests on 5.0 GHz radios
  - <0-10000> – Specify a client probe request threshold from 0 - 100000.

- **probe-req-intvl [2.4Ghz|5Ghz] <0-10000>**
  - Optional. Configures client probe request interval limits for device association
  - 2.4GHz – Configures the client probe request interval on 2.4 GHz radios
  - 5GHz – Configures the client probe request interval on 5.0 GHz radios
  - <0-10000> – Specify a value from 0 - 100000.
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
crypton-type none
authentication-type eap
accounting syslog host 172.16.10.4 port 2
client-load-balancing probe-req-intvl 5ghz 5
captive-portal-enforcement fall-back
acl exceed-rate wireless-client-denied-traffic 20 disassociate
broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
4.1.70.2.13 controller-assisted-mobility

**wlan-mode commands**

Enables controller or service platform assisted mobility to determine a wireless client’s VLAN assignment.

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, NX9000, NX9500, NX9510, NX9600

**Syntax**

controller-assisted-mobility

**Parameters**

None

**Examples**

```
rfs4000-229D58(config-wlan-test)#controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

```
rfs4000-229D58(config-wlan-test)#show context
wlan test
SSID test
bridging-mode tunnel
encryption-type none
authentication-type none
controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```
4.1.70.2.14 data-rates

Specifies the 802.11 rates supported on a WLAN

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
data-rates [2.4GHz|5GHz]
data-rates 2.4GHz [b-only|bg|bgn|custom|default|g-only|gn]
data-rates 2.4GHz custom [1|11|12|18|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]
```

<table>
<thead>
<tr>
<th>data-rates</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>

```
data-rates 5GHz [a-only|an|default]
```

<table>
<thead>
<tr>
<th>data-rates</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>
<tr>
<td>data-rates [2.4GHz</td>
<td>5GHz] custom [1</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>data-rates [2.4GHz</td>
<td>5GHz]</td>
</tr>
<tr>
<td>custom</td>
<td>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.</td>
</tr>
<tr>
<td>1,11,2, 5.5</td>
<td>The following data rates are specific to the 2.4 GHz channel:</td>
</tr>
<tr>
<td>• 1 – 1-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 11 – 11-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 2 – 2-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 5.5 – 5.5-Mbps</td>
<td></td>
</tr>
<tr>
<td>[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]</td>
<td>The following data rates are common to both the 2.4 GHz and 5.0 GHz channels:</td>
</tr>
<tr>
<td>• 12 – 12 Mbps</td>
<td></td>
</tr>
<tr>
<td>• 18 – 18-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 24 – 24 Mbps</td>
<td></td>
</tr>
<tr>
<td>• 36 – 36-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 48 – 48-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 54 – 54-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 6 – 6-Mbps</td>
<td></td>
</tr>
<tr>
<td>• 9 – 9-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-1 – basic 1-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-11 – basic 11-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-12 – basic 12-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-18 – basic 18-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-2 – basic 2-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-36 – basic 36-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-48 – basic 48-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-5.5 – basic 5.5-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-54 – basic 54-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-6 – basic 6-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-9 – basic 9-Mbps</td>
<td></td>
</tr>
<tr>
<td>• basic-mcs-1s – Modulation and coding scheme data rates for 1 Spatial Stream</td>
<td></td>
</tr>
<tr>
<td>• mcs-1s – Applicable to 1-spatial stream data rates</td>
<td></td>
</tr>
<tr>
<td>• mcs-2s – Applicable to 2-spatial stream data rates</td>
<td></td>
</tr>
<tr>
<td>• mcs-3s – Applicable to 3-spatial stream data rates</td>
<td></td>
</tr>
</tbody>
</table>
Examples

```
?fs7000-37FABE(config-wlan-test)#data-rates 2.4GHz gn

?fs7000-37FABE(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
?fs7000-37FABE(config-wlan-test)#
```
4.1.70.2.15 description

Defines the WLAN description

Supported in the following platforms:

- Access Points — AP300, 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, 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>The WLAN's description should help differentiate it from others with similar configurations. The description should not exceed 64 characters.</td>
<td></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)#

```
4.1.70.2.16 downstream-group-addressed-forwarding

- wlan-mode commands

Enables/disables forwarding of downstream BCMC packets to a group on this WLAN. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, 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)#
4.1.70.2.17 dynamic-vlan-assignment

wlan-mode commands

Configures dynamic VLAN assignment on this WLAN

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

dynamic-vlan-assignment allowed-vlan <VLAN-ID>

Parameters

- dynamic-vlan-assignment allowed-vlan <VLAN-ID>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowed-vlan &lt;VLAN-ID&gt;</td>
<td>Configures a list of VLAN IDs or VLAN alias allowed access to the WLAN</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-wlan-test)#dynamic-vlan-assignment allowed-vlan 10-20
rfs4000-229D58(config-wlan-test)#

rfs4000-229D58(config-wlan-test)#show context
wlan test
  ssid test
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  dynamic-vlan-assignment allowed-vlan 10-20
rfs4000-229D58(config-wlan-test)#
### 4.1.70.2.18 eap-types

**wlan-mode commands**

Configures client access based on the EAP type used

Supported in the following platforms:

- Access Points — AP300, 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, 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]{aka|all|fast|peap|sim|tls|ttls}**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap-types</td>
<td>Configures a list of allowed or denied EAP types</td>
</tr>
<tr>
<td>[allow</td>
<td>deny]</td>
</tr>
<tr>
<td>[aka</td>
<td>all</td>
</tr>
</tbody>
</table>

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
- **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 (GSME) 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 Tunnelled 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)#
### 4.1.70.2.19 encryption-type

Sets a WLAN's encryption type

Supported in the following platforms:

- **Access Points** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, 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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmp</td>
<td>Configures <strong>Advanced Encryption Standard</strong> (AES) <strong>Counter Mode CBC-MAC Protocol</strong> (AES-CCM/CCMP)</td>
</tr>
<tr>
<td>keyguard</td>
<td>Configures Keyguard-MCM (Mobile Computing Mode)</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
capture-portal-enforcement fall-back
acl exceed-rate wireless-client-denied-traffic 20 disassociate
broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
```
4.1.70.2.20 enforce-dhcp

**wlan-mode commands**

Drops packets from clients with a static IP address

Supported in the following platforms:
- Access Points — AP300, 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, 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-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
enforce-dhcp
broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-test)#
4.1.70.2.21 fast-bss-transition

wlan-mode commands

Enables or disables 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
fast-bss-transition

Parameters
None

Examples
rfs7000-37FABE(config-wlan-test)#fast-bss-transition
rfs7000-37FABE(config-wlan-test)#
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)#
4.1.70.2.22 http-analyze

* wlan-mode commands

Enables HTTP URL analysis on the WLAN

Supported in the following platforms:
- Access Points — AP300, 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, 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]}**
  - **syslog** Forwards client and URL information to a syslog server
    - **host <IP/HOSTNAME>** — Specify the syslog server’s IP address or hostname
    - **port <1-65535>** Optional. Specifies the UDP port to connect to the syslog server from 1 - 65535
    - **proxy-mode [none|through-controller|through-rf-domain-manager]** Optional. Specifies if the request is to be proxied through another device
      - **none** — Requests are sent directly to syslog server from device
      - **through-controller** — Proxies requests, to the syslog server, through the controller configuring the device
      - **through-rf-domain-manager** — Proxies requests, to the syslog server, through the local 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
rfs4000-229D58(config-wlan-test)#http-analyze syslog host 192.168.13.10 port 21 proxy-mode through-controller
rfs4000-229D58(config-wlan-test)#
```
4.1.70.2.23 ip

- **wlan-mode commands**

  Configures Internet Protocol (IP) settings

  **Supported in the following platforms:**
  - Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

  **Syntax**

  ip [arp|dhcp]

  ip arp [header-mismatch-validation|trust]

  ip dhcp trust

  **Parameters**

  - ip arp [header-mismatch-validation|trust]
    - **ip arp** Configures the IP settings for ARP packets
    - **header-mismatch-validation** Verifies mismatch of source MAC address in the ARP and Ethernet headers
    - **trust** Sets ARP responses as trusted for a WLAN/range

  - ip dhcp trust
    - **ip dhcp** Configures the IP settings for DHCP packets
    - **trust** Sets DHCP responses as trusted for a WLAN/range

  **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)#
4.1.70.2.24 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 — AP300, 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, 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 password 0 <LINE> — Configures a clear text password

  kerberos password 2 <LINE> — Configures an encrypted password

  kerberos password <LINE> — Specify the password.

- kerberos realm <REALM>

  kerberos realm — Configures a Kerberos KDC server realm. The REALM should not exceed 127 characters.

- kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}

  kerberos server — Configures a Kerberos server's IP address and port number.

  kerberos server primary — Configures the primary server.

  kerberos server secondary — Configures the secondary server.

  kerberos server timeout — Configures the timeout value for the server connection.
server [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>  Sets the primary or secondary KDC server address
- <IP/HOSTNAME> – Specify the IP address or name of the KDC server.

port <1-65535>  Optional. Configures the UDP port used to connect to the KDC server
- <1-65535> – Specify the port from 1 - 65535. The default is 88.

- kerberos server timeout <1-60>

kerberos  Configures a WLAN’s Kerberos authentication parameters
The parameters are: password, realm, and server.

timeout <1-60>  Modifies the Kerberos KDC server’s timeout parameters
- <1-60> – Specifies the wait time for a response from the Kerberos KDC server before retrying. Specify a value from 1 - 60 seconds.

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)#
4.1.70.2.25 mac-authentication

+wlan-mode commands

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
mac-authentication cached-credentials

Parameters
- mac-authentication cached-credentials

| mac-authentication cached-credentials | Uses cached credentials to skip RADIUS lookups |

Examples
rfs4000-229D58 (config-wlan-test)#mac-authentication cached-credentials
rfs4000-229D58 (config-wlan-test)#
### 4.1.70.2.26 mac-registration

**wlan-mode commands**

Enables dynamic MAC registration of a user

**NOTE:** This feature is supported only if MAC authentication is enabled. To enable MAC authentication use the `authentication-type > mac` command in the config WLAN mode.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mac-registration [external|group-name]
mac-registration external host <IP/HOSTNAME> {proxy-mode [none|through-controller|through-rf-domain-manager]}
mac-registration group-name <GROUP-NAME> {agreement-refresh <0-100>|expiry-time <1-1500>}
```

**Parameters**

- **mac-registration external host <IP/HOSTNAME> {proxy-mode [none|through-controller|through-rf-domain-manager]}
  - Optional. Specifies the forwarding mode
  - *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* – Requests are proxied through the local RF Domain manager

- **mac-registration group-name <GROUP-NAME> {agreement-refresh <0-100>|expiry-time <1-1500>}
  - Optional. Specifies the user expiry time in days from 1 - 1500
  - *<GROUP-NAME>* – Specify the group name.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-registration</td>
<td>Enables dynamic MAC registration of a user</td>
</tr>
<tr>
<td>external</td>
<td>Forwards MAC registration user information to the external controller</td>
</tr>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Specifies the external controller's IP address or hostname</td>
</tr>
<tr>
<td>proxy-mode</td>
<td>Optional. Specifies the forwarding mode</td>
</tr>
<tr>
<td>through-controller</td>
<td><em>none</em> – Requests are sent directly to the controller from the requesting device</td>
</tr>
<tr>
<td>through-rf-domain</td>
<td><em>through-controller</em> – Requests are proxied through the controller configuring the device</td>
</tr>
<tr>
<td>through-rf-domain</td>
<td><em>through-rf-domain</em> – Requests are proxied through the local RF Domain manager</td>
</tr>
<tr>
<td>group-name</td>
<td>Specifies the group to which the MAC registered user should be added</td>
</tr>
<tr>
<td>&lt;GROUP-NAME&gt;</td>
<td><em>&lt;GROUP-NAME&gt;</em> – Specify the group name.</td>
</tr>
<tr>
<td>expiry-time &lt;1-1500&gt;</td>
<td>Optional. Specifies the user expiry time in days from 1 - 1500</td>
</tr>
<tr>
<td>agreement-refresh</td>
<td>Optional. Sets the time (in days), after which an inactive user has to refresh the WLAN's terms of agreement. For example, if the agreement refresh period is set to 10, a user logging in after 10 days of inactivity will be displayed the agreement page. and will be allowed WLAN access only after refreshing the terms of agreement.</td>
</tr>
<tr>
<td>&lt;0-100&gt;</td>
<td><em>&lt;0-100&gt;</em> – Specify the number of days from 0 - 100.</td>
</tr>
</tbody>
</table>
Examples

```bash
rfs7000-37FABE(config-wlan-1)#mac-registration group-name test expiry-time 100

rfs7000-37FABE(config-wlan-1)#mac-registration external host 172.16.10.8 proxy-mode through-controller
rfs7000-37FABE(config-wlan-1)#show context
  wlan 1
    ssid 1
    bridging-mode tunnel
    encryption-type none
    authentication-type mac
    mac-registration group-name test expiry-time 100
    mac-registration external host 172.16.10.8 proxy-mode through-controller
rfs7000-37FABE(config-wlan-1)#

rfs4000-229D58(config-wlan-wlan-testing)#mac-registration group-name Group3 ?
  agreement-refresh Specify when the agreement page should be displayed to
                     the user (in days)
  expiry-time     Specify the user expiry time in days
<cr>
rfs4000-229D58(config-wlan-wlan-testing)#

rfs4000-229D58(config-wlan-wlan-testing)#mac-registration group-name Group3 agreement-refresh ?
  <0-100> Agreement page will be displayed to the user if the user has not
           visited in the past (number of days)
<cr>
rfs4000-229D58(config-wlan-wlan-testing)#

rfs4000-229D58(config-wlan-wlan-testing)#mac-registration group-name Group3 agreement-refresh 19
```
### 4.1.70.2.27 wing-extensions

**wlan-mode commands**

Enables support for WiNG specific extensions to 802.11

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wing-extensions [move-command|smart-scan|wing-load-information|wmm-load-information]
```

**Parameters**

- **wing-extensions [move-command|smart-scan|wing-load-information|wmm-load-information]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wing-extensions</td>
<td>Enables support for WiNG specific extensions to 802.11</td>
</tr>
<tr>
<td>move-command</td>
<td>Enables support for WiNG move (fast roaming) feature</td>
</tr>
<tr>
<td>smart-scan</td>
<td>Enables support for smart scanning feature</td>
</tr>
<tr>
<td>wing-load-information</td>
<td>Enables support for the WiNG load information element (Element ID 173)</td>
</tr>
<tr>
<td>wmm-load-information</td>
<td>Enables support for the WiNG WMM load information element</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-wlan-test)#wing-extensions wmm-load-information
```

```
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
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)#
```
4.1.70.2.28 no

▶ wlan-mode commands

Negates WLAN mode commands and reverts values to their default

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
no <PARAMETER>

Parameters
None

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
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
ccontroller-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
eap-types Allow all EAP types on this wlan
encryption-type Reset the encryption to use on this wlan to default (none)
enforce-dhcp Drop packets from Wireless Clients with static IP address
fast-bss-transition Disable support for 802.11r Fast BSS Transition
http-analyze Enable HTTP URL analysis on the wlan
ip Internet Protocol (IP)
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>mac-registration</td>
<td>Dynamic MAC registration of user</td>
</tr>
<tr>
<td>wing-extensions</td>
<td>Disable support for WiNG-Specific extensions to 802.11</td>
</tr>
<tr>
<td>protected-mgmt-frames</td>
<td>Disable support for Protected Management Frames (IEEE 802.11w)</td>
</tr>
<tr>
<td>proxy-arp-mode</td>
<td>Configure handling of ARP requests with proxy-arp is enabled</td>
</tr>
<tr>
<td>radio-resource-measurement</td>
<td>Disable support for 802.11k Radio Resource Measurement</td>
</tr>
<tr>
<td>radius</td>
<td>Configure RADIUS related parameters</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>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>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>

```
rfs7000-37FABE(config-wlan-test)#

The test settings before execution of the no command:

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
endeforce-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
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)#
4.1.70.2.29 proxy-arp-mode

* wlan-mode commands

Enables proxy ARP mode for handling ARP requests

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

proxy-arp-mode [dynamic|strict]

Parameters

- proxy-arp-mode [dynamic|strict]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Forwards ARP requests to the wireless side (for which a response could not be proxied)</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)#
4.1.70.2.30 radio-resource-measurement

**wlan-mode commands**

Enables support for 802.11k radio resource measurement

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
radio-resource-measurement {channel-report}
```

**Parameters**

- `radio-resource-measurement {channel-report}`

<table>
<thead>
<tr>
<th>radio-resource-measurement {channel-report}</th>
<th>Enables support for 802.11k radio resource measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• channel-report – Optional. Includes the channel-report element in beacons and probe responses</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs4000-229D58(config-wlan-test)#radio-resource-measurement
rfs4000-229D58(config-wlan-test)#

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)#
```
4.1.70.2.31 radius

- wlan-mode commands

Configures RADIUS related parameters

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>dynamic-authorization</th>
<th>Enables support for disconnect and change of authorization messages (RFC5176)</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas-identifier &lt;NAS-ID&gt;</td>
<td>Configures the WLAN NAS identifier sent to the RADIUS server. The NAS identifier should not exceed 256 characters.</td>
</tr>
<tr>
<td>nas-port-id &lt;NAS-PORT-ID&gt;</td>
<td>Configures the WLAN NAS port ID sent to the RADIUS server. The NAS port identifier should not exceed 256 characters.</td>
</tr>
<tr>
<td>vlan-assignment</td>
<td>Configures the VLAN assignment of a WLAN. When enabled, this option assigns clients to the RADIUS server specified VLANs. This option is disabled by default.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-wlan-test)#radius vlan-assignment

erfs7000-37FABE(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
http-analyze controller
erfs7000-37FABE(config-wlan-test)#
4.1.70.2.32 relay-agent

Enables support for DHCP relay agent information (option 82) feature on this WLAN

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
relay-agent dhcp-option82

Parameters
- relay-agent dhcp-option82

<table>
<thead>
<tr>
<th>relay-agent</th>
<th>dhcp-option82</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports DHCP option 82. When enabled, this feature allows the DHCP relay agent to insert the relay agent information option (option 82) in client requests forwarded to the DHCP server. This information provides the following:</td>
<td></td>
</tr>
<tr>
<td>• circuit ID suboption – Provides the SNMP port interface index</td>
<td></td>
</tr>
<tr>
<td>• remote ID – Provides the controller’s MAC address</td>
<td></td>
</tr>
</tbody>
</table>

Examples
rfs4000-229D58 (config-wlan-test)#relay-agent dhcp-option82
rfs4000-229D58 (config-wlan-test)#

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)#
### 4.1.70.2.33 shutdown

**wlan-mode commands**

Shuts down a WLAN

Supported in the following platforms:

- **Access Points** — AP300, 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, 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><strong>Shutdown</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown</td>
<td>Shuts down the WLAN when specified events occur. Disabled by default.</td>
</tr>
<tr>
<td>on-critical-resource</td>
<td>Optional. Shuts down the WLAN when critical resource failure occurs. Disabled by default.</td>
</tr>
<tr>
<td>on-meshpoint-loss</td>
<td>Optional. 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. 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. 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**

```bash
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)#
```
**4.1.70.2.34 ssid**

* wlan-mode commands

Configures a WLAN's SSID

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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**

```plaintext
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)#
```
4.1.70.2.35 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax:

```
time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start <START-TIME>} [end <END-TIME>]
```

Parameters:
- `time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start <START-TIME>} [end <END-TIME>]`

<table>
<thead>
<tr>
<th>day &lt;option&gt;</th>
<th>Specifies the day or days on which the client can access the WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>sunday</td>
<td>Allows access on Sundays only</td>
</tr>
<tr>
<td>monday</td>
<td>Allows access on Mondays only</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Allows access on Tuesdays only</td>
</tr>
<tr>
<td>wednesday</td>
<td>Allows access on Wednesdays only</td>
</tr>
<tr>
<td>thursday</td>
<td>Allows access on Thursdays only</td>
</tr>
<tr>
<td>friday</td>
<td>Allows access on Fridays only</td>
</tr>
<tr>
<td>saturday</td>
<td>Allows access on Saturdays only</td>
</tr>
<tr>
<td>weekends</td>
<td>Allows access on weekends only</td>
</tr>
<tr>
<td>weekdays</td>
<td>Allows access on weekdays only</td>
</tr>
<tr>
<td>all</td>
<td>Allows access on all days</td>
</tr>
</tbody>
</table>

- `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
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
--More--
rfs7000-37FABE(config-wlan-test)#
```
4.1.70.2.36 use

**wlan-mode commands**

This command associates an existing captive portal with a WLAN.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use [aaa-policy|association-acl-policy|bonjour-gw-discovery-policy|captive-portal|
ip-access-list|mac-access-list|passpoint-policy|wlan-qos-policy]
use [aaa-policy <AAA-POLICY-NAME>|association-acl-policy <ASSOCIATION-POLICY-NAME>|
bonjour-gw-discovery-policy <POLICY-NAME>|captive-portal <CAPTIVE-PORTAL-NAME>|
passpoint-policy <PASSPOINT-POLICY-NAME>|wlan-qos-policy <WLAN-QoS-POLICY-NAME>]
use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>
```

**Parameters**

- **aaa-policy <AAA-POLICY-NAME>** Uses an existing AAA policy with a WLAN
  - `<AAA-POLICY-NAME>` — Specify the AAA policy name.

- **association-acl <ASSOCIATION-POLICY-NAME>** Uses an existing association ACL policy with a WLAN
  - `<ASSOCIATION-POLICY-NAME>` — Specify the association ACL policy name.

- **bonjour-gw-discovery-policy <POLICY-NAME>** Uses an existing Bonjour GW Discovery policy with a WLAN. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming over WLAN.
  - `<POLICY-NAME>` — Specify the Bonjour GW Discovery policy name (should be existing and configured).
  **Note:** In the WiNG network, this feature is supported only on the RFS7000 and AP7131 devices.
  **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.
**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)#
4.1.70.2.37 vlan

Sets the VLAN where traffic from a WLAN is mapped

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

Parameters
- `<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 be pre-existing and configured VLAN.

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)#
```
4.1.70.2.38 vlan-pool-member

* wlan-mode commands

Adds a member VLAN to a WLAN’s VLAN pool

---

**NOTE:** Configuration of a VLAN pool overrides the ‘vlan’ configuration.

---

Supported in the following platforms:
- Access Points — AP300, 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, 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>&lt;WORD&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><code>limit &lt;0-8192&gt;</code></td>
<td>Optional. Is ignored if the number of clients are limited and well within the limits of the DHCP pool on the VLAN. The <code>&lt;0-8192&gt;</code> specifies the number of users allowed.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-wlan-test)#vlan-pool-member 1-10 limit 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
radius vlan-assignment
time-based-access days weekdays start 10:00 end 16:30
wing-extensions wmm-load-information
--More--
rfs7000-37FABE(config-wlan-test)#
```

---

**NOTE:**
Configuration of a VLAN pool overrides the ‘vlan’ configuration.
4.1.70.2.39 wep128

wlan-mode commands

Configures WEP128 parameters

Supported in the following platforms:
- Access Points — AP300, 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, 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>]
  - wep128 Configures WEP128 parameters. The parameters are: key, key-from-passkey, and transmit-key.
  - key <1-4> 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>
  - keys-from-passkey Specifies a passphrase from which keys are derived
    - <WORD> – Specify a passphrase from 4 - 32 characters.
- wep128 transmit-key <1-4>
  - 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 company@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)#
4.1.70.2.40 wep64

- wlan-mode commands

Configures WEP64 parameters

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
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>]` — Configures 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 key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128)

  - **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 the key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters 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 testr

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 6d6f746f72
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)#
4.1.70.2.41 wireless-client

- wlan-mode commands

Configures the transmit power indicated to clients

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

wireless-client [count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|max-firewall-sessions|reauthentication|roam-notification|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>|tx-power <0-20>|vlan-cache-ageout <60-86400>]

wireless-client roam-notification [after-association|after-data-ready|auto]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count-per-radio &lt;0-256&gt;</td>
<td>Configures the maximum number of clients allowed on this WLAN per radio</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-256&gt; – Specify a value from 0 - 256.</td>
</tr>
<tr>
<td>cred-cache-ageout &lt;60-86400&gt;</td>
<td>Configures the timeout period for which client credentials are cached across associations</td>
</tr>
<tr>
<td></td>
<td>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds.</td>
</tr>
<tr>
<td>hold-time &lt;1-86400&gt;</td>
<td>Configures the time period for which wireless client state information is cached post roaming</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-86400&gt; – Specify a value from 1 - 86400 seconds.</td>
</tr>
<tr>
<td>inactivity-timeout &lt;60-86400&gt;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds.</td>
</tr>
<tr>
<td>max-firewall-sessions &lt;10-10000&gt;</td>
<td>Configures the maximum firewall sessions allowed per client on a WLAN</td>
</tr>
<tr>
<td></td>
<td>• &lt;10-10000&gt; – Specify the maximum number of firewall sessions allowed from 10 - 10000.</td>
</tr>
<tr>
<td>reauthentication &lt;30-86400&gt;</td>
<td>Configures periodic reauthentication of associated clients</td>
</tr>
<tr>
<td></td>
<td>• &lt;30-86400&gt; – Specify the client reauthentication interval from 30 - 86400 seconds.</td>
</tr>
<tr>
<td>tx-power &lt;0-20&gt;</td>
<td>Configures the transmit power indicated to clients</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-20&gt; – Specify a value from 0 - 20 dBm.</td>
</tr>
<tr>
<td>vlan-cache-ageout &lt;60-86400&gt;</td>
<td>Configures the timeout period for which client VLAN information is cached across associations.</td>
</tr>
<tr>
<td></td>
<td>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds.</td>
</tr>
</tbody>
</table>
- **wireless-client roam-notification [after-association|after-data-ready|auto]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless-client</td>
<td>Configures the transmit power indicated to wireless clients for transmission</td>
</tr>
<tr>
<td>roam-notification</td>
<td>Configures when a roam notification is transmitted</td>
</tr>
<tr>
<td>after-association</td>
<td>Transmits a roam notification after a client has associated</td>
</tr>
<tr>
<td>after-data-ready</td>
<td>Transmits a roam notification after a client is data-ready (after completion of authentication, handshakes etc.)</td>
</tr>
<tr>
<td>auto</td>
<td>Transmits a roam notification upon client association (if the client is known to have authenticated to the network)</td>
</tr>
</tbody>
</table>

**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
  wep64 key 1 hex 0 6d6f746f72
  wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
  wep128 key 2 hex 0 2b3fb36924b222dffe98c86c315
  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
  wmm-load-information
  wireless-client tx-power 12
  client-load-balancing probe-req-intvl 5ghz 5
--More--
```

rfs7000-37FABE(config-wlan-test)#
### 4.1.70.2.42 wpa-wpa2

**wlan-mode commands**

Modifies TKIP-CCMP (WPA/WPA2) related parameters

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
wpa-wpa2 [exclude-wpa2-tkip|handshake|key-rotation|opp-pmk-caching|pmk-caching|preauthentication|psk|tkip-countermeasures|use-sha256-akm]
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|use-sha256-akm]
wpa-wpa2 handshake [attempts|init-wait|priority|timeout]
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]|timeout <10-5000> {10-5000}]
wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>
wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]
wpa-wpa2 tkip-countermeasures holdtime <0-65535>
```

**Parameters**

- **wpa-wpa2** [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wpa-wpa2</td>
<td>Modifies TKIP-CCMP (WPA/WPA2) related parameters</td>
</tr>
<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.</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</td>
</tr>
<tr>
<td>pmk-caching</td>
<td>Uses cached pair-wise master keys (fast roaming with eap/802.1x)</td>
</tr>
<tr>
<td>preauthentication</td>
<td>Uses pre-authentication mode (WPA2 fast roaming)</td>
</tr>
<tr>
<td>use-sha256-akm</td>
<td>Uses sha256 authentication key management suite</td>
</tr>
<tr>
<td>wpa-wpa2 handshake</td>
<td>Configures WPA/WPA2 handshake parameters</td>
</tr>
<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.</td>
</tr>
<tr>
<td>init-wait &lt;5-1000000&gt;</td>
<td>Configures a minimum wait-time period, in microseconds, before the first handshake message is transmitted from the AP</td>
</tr>
<tr>
<td></td>
<td>• &lt;5-1000000&gt; – Specify a value from 5 - 1000000 microseconds.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>wpa-wpa2</code></td>
<td>Modifies TKIP-CCMP (WPA/WPA2) related parameters</td>
</tr>
<tr>
<td><code>key-rotation</code></td>
<td>Configures parameters related to periodic rotation of encryption keys. The periodic key rotation parameters are broadcast, multicast, and unicast traffic.</td>
</tr>
<tr>
<td><code>broadcast</code></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.</td>
</tr>
<tr>
<td><code>&lt;30-86400&gt;</code></td>
<td>Specify a value from 30 - 86400 seconds.</td>
</tr>
<tr>
<td><code>unicast</code></td>
<td>Configures a periodic interval for the rotation of keys, used for unicast traffic</td>
</tr>
<tr>
<td><code>&lt;30-86400&gt;</code></td>
<td>Specify a value from 30 - 86400 seconds.</td>
</tr>
<tr>
<td><code>psk</code></td>
<td>Configures a pre-shared key. The key options are: 0, 2, and LINE</td>
</tr>
<tr>
<td><code>0 &lt;LINE&gt;</code></td>
<td>Configures a clear text key</td>
</tr>
<tr>
<td><code>2 &lt;LINE&gt;</code></td>
<td>Configures an encrypted key</td>
</tr>
<tr>
<td><code>&lt;LINE&gt;</code></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><code>tkip-countermeasures holdtime</code></td>
<td>Configures a hold time period for implementation of TKIP counter measures</td>
</tr>
<tr>
<td><code>&lt;0-65535&gt;</code></td>
<td>Specify a value from 0 - 65536 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
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 6d6f746f72
wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
--More--
rfs7000-37FABE(config-wlan-test)#
4.1.70.2.43 service

wlan-mode commands

Invokes service commands applicable in the WLAN configuration mode

Supported in the following platforms:
- Access Points — AP300, 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, 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|tx-deauth-on-roam-detection|unresponsive-client|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-throttle <0-254>

service eap-mac-mode [mac-always|normal]

service key-index eap-wep-unicast <1-4>

service monitor [aaa-server|adoption|captive-portal|dhcp|dns]

service [dhcp|dns] crm <CRM-POLICY-NAME> vlan <1-4094>

service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]

service unresponsive-client [attempts <1-1000>|timeout <1-60>]

Parameters

- 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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-ht-only</td>
<td>Only allows clients capable of High Throughput (802.11n) data rates to associate</td>
</tr>
<tr>
<td>allow-open-passpoint</td>
<td>Enables non-WPA2 security for passpoint WLANs. For more information on passpoint policy and configuration, see PASSPOINT POLICY.</td>
</tr>
<tr>
<td>cred-cache clear-on-disconnect</td>
<td>Clears credential cache after a client has disconnected from the network</td>
</tr>
<tr>
<td>eap-mac-multicopy</td>
<td>Enables sending of multiple copies of broadcast and unicast messages</td>
</tr>
<tr>
<td>eap-mac-multikeys</td>
<td>Enables configuration of different key indices for MAC authentication</td>
</tr>
<tr>
<td>enforce-pmkid-validation</td>
<td>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 EIEEE 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.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radio-crypto</td>
<td>Uses radio hardware for encryption and decryption. This is applicable only for devices using Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (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>seamless</td>
<td></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>
<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>
<tr>
<td>eap-throttle &lt;0-254&gt;</td>
<td>Enables EAP request throttling. This command allows you 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>key-index eap-wep-unicast &lt;1-4&gt;</td>
<td>Configures an index with each key during EAP authentication with WEP</td>
</tr>
<tr>
<td>monitor [aaa-server</td>
<td>adoption vlan &lt;1-4094&gt;</td>
</tr>
<tr>
<td>aaa-server’</td>
<td>Enables AAA server failure monitoring. This feature is disabled by default.</td>
</tr>
<tr>
<td>adoption vlan &lt;1-4094&gt;</td>
<td>Enables adoption failure monitoring on an adopted AP. Also configures a adoption failover VLAN. This feature is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• VLAN &lt;1-4094&gt; – Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost.</td>
</tr>
</tbody>
</table>

Contd.......
GLOBAL CONFIGURATION COMMANDS

**service monitor [dhcp|dns] crm <CRM-POLICY-NAME> vlan <1-4094>**

*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).

**service unresponsive-client [attempts <1-1000>|timeout <1-60>]**

*Note:* Configures handling of unresponsive clients

- **attempts <1-1000>** — Specify a value from 1 - 1000.
- **timeout <1-60>** — Specify a value from 1 - 60 seconds.

**service monitor [dhcp|dns] crm <CRM-POLICY-NAME> vlan <1-4094>**

*Note:* Enables DHCP and/or DNS server monitoring service on this WLAN. To enable DHCP server monitoring, associate an existing critical-resource monitoring (CRM) policy with this WLAN. For more information on CRM policy creation, see critical-resource.

- **crm <CRM-POLICY-NAME>** — Specify the name of the critical-resource monitoring policy created.
- **VLAN <1-4094>** — Configures the failover VLAN from 1 - 4094. This is the VLAN on which clients are mapped when the connectivity between the AAP and the controller is lost.

*Note:* Once enabled, the CRM server monitors the DHCP/DNS server and updates their status as 'up' or 'down' depending on the reachability 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.

**eap-mac-mode**

Enables external captive portal server failure monitoring. 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.

**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)#
```
### 4.1.71 wlan-qos-policy

**Global Configuration Commands**

Configures a WLAN QoS policy

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`wlan-qos-policy <WLAN-QOS-POLICY-NAME>`

**Parameters**

- `wlan-qos-policy <WLAN-QOS-POLICY-NAME>`

**Examples**

```
show wlan-qos-policy test
show wlan-qos-policy 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`: Clears the display screen
- `commit`: Commit all changes made in this session
- `do`: Run commands from Exec mode
- `end`: Exit 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:** For more information on WLAN QoS policy commands, see Chapter 22, WLAN-QOS-POLICY.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes an existing WLAN QoS Policy</td>
</tr>
</tbody>
</table>
4.1.72 smart-cache-policy

Global Configuration Commands

Table 4.20 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 4-287</td>
</tr>
<tr>
<td>smart-cache-policy-mode</td>
<td>Summarizes the smart cache policy configuration mode commands</td>
<td>page 4-289</td>
</tr>
</tbody>
</table>
4.1.72.1 smart-cache-policy

This command 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.

---

**NOTE:** Content caching is a licensed feature, supported only on the NX45XX and NX65XX series service platforms. To enable content caching on a device, use the license command (in the device-config mode) and provide the SMART-CACHE license key. For more information, see [license].

**NOTE:** Though the NX9000 series service platforms do not support content caching, they support the configuration of smart-content caching policies that can be applied to the NX45XX and NX65XX series service platforms. The NX9000 series service platforms are capable of adopting and configuring NX45XX and NX65XX series service platforms.

---

Supported in the following platforms:
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**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
  service     
  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)#
### 4.1.72.2 smart-cache-policy-mode commands

*smart-cache-policy*

Table 4.21 summarises 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 4-290</td>
</tr>
<tr>
<td>aging</td>
<td>Configures the refresh pattern (aging parameters) for specific content types</td>
<td>page 4-291</td>
</tr>
<tr>
<td>cache</td>
<td>Configures cache management settings</td>
<td>page 4-293</td>
</tr>
<tr>
<td>forward-proxy</td>
<td>Configures the address and port for forward caching proxy service</td>
<td>page 4-295</td>
</tr>
<tr>
<td>http-access</td>
<td>Configures HTTP filters – <em>access control lists</em> (ACLs)</td>
<td>page 4-297</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets content cache policy settings</td>
<td>page 4-299</td>
</tr>
<tr>
<td>pre-fetch</td>
<td>Enables pre fetching of URL lists</td>
<td>page 4-300</td>
</tr>
<tr>
<td>parent-proxy</td>
<td>Enables/disables parent proxy on this smart cache policy</td>
<td>page 4-301</td>
</tr>
<tr>
<td>smart-cache</td>
<td>Enables smart content caching</td>
<td>page 4-302</td>
</tr>
<tr>
<td>transparent-proxy</td>
<td>Configures transparent caching proxy settings</td>
<td>page 4-303</td>
</tr>
</tbody>
</table>
4.1.72.2.1 access-log

*smart-cache-policy-mode commands*

Enables or disables 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, NX6500, NX6524, 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>
<tbody>
<tr>
<td><code>rotate &lt;0-10&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;0-10&gt;</code> — Optional. Specify the number of rotations from 0 - 10. The default is 10 rotations on every 1 MB.</td>
</tr>
<tr>
<td><code>rotate-type</code></td>
<td>Optional. Configures access log file rotation conditions, such as duration and size</td>
</tr>
<tr>
<td></td>
<td>- <code>duration &lt;1-100&gt;</code> — Rotates log files by time. Specify the time from 1 - 100 days. The default is 1 day.</td>
</tr>
<tr>
<td></td>
<td>- <code>size &lt;1-100&gt;</code> — Rotates log files by file size. Specify the size from 1 - 100 MB.</td>
</tr>
</tbody>
</table>

**Examples**

```
nx4500-5CFA2B(config-smart-cache-policy-test)#access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
nx4500-5CFA2B(config-smart-cache-policy-test)#show context smart-cache-policy test
access-log rotate 10 rotate-type duration 10 day
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

**Related Commands**

- `no` Disables client request logging
4.1.72.2 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, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

```
ageing precedence <1-100> [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>**
  - Configures content cache aging rules and assigns a precedence to each rule
  - **precedence <1-100>** – Specify a precedence for this aging rule.
- **<WORD>**
  - Specifies the regular expression to match. This option is case sensitive, and is the default setting.
- **ignore-case <WORD>**
  - Specifies the regular expression to match. This option is not case sensitive.
- **min-age <0-525600>**
  - 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.
  - **<0-525600>** – Specify a value from 0 - 525600 minutes. The default is 1 minute.
- **freshness-factor <0-100>**
  - 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.
  - **<0-100>** – Specify a value from 0 - 100%. The default is 100%.
- **max-age <0-525600>**
  - 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.
  - **<0-525600>** – Specify a value from 0 - 525600 minutes. The default is 525600.
### Examples

```bash
nx4500-5CFA2B(config-smart-cache-policy-test)#aging precedence 1 ignore-case \\.jpg$
min-age 100 freshness-factor 75 max-age 200 reload-into-ims

nx4500-5CFA2B(config-smart-cache-policy-test)#
```

```bash
nx4500-5CFA2B(config-smart-cache-policy-test)#show context
smart-cache-policy test
  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)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an existing aging rule (refresh pattern)</td>
</tr>
</tbody>
</table>
4.1.72.2.3 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, NX6500, NX6524, 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\>|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></td>
<td>• aol.com</td>
</tr>
<tr>
<td></td>
<td>• bing.com</td>
</tr>
<tr>
<td></td>
<td>• break.com</td>
</tr>
<tr>
<td></td>
<td>• dailymotion.com</td>
</tr>
<tr>
<td></td>
<td>• metacafe.com</td>
</tr>
<tr>
<td></td>
<td>• vimeo.com</td>
</tr>
<tr>
<td></td>
<td>• cnn.com</td>
</tr>
<tr>
<td></td>
<td>• youtube.com</td>
</tr>
</tbody>
</table>

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.

- cache precedence <1-100> [deny|permit] \{destination-domain <DOMAIN-NAME>|destination-domain-regex \<WORD\>|destination-ip \(<IP>/M|any\)|source-ip \<IP\>|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></td>
<td>• &lt;1-100&gt; – Specify a precedence rule from 1 - 100.</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 |
### cache size <1-32>

Configures the maximum caching storage size. This is 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.

### Examples

```bash
nx4500-5CFA2B(config-smart-cache-policy-test)#cache size 30
nx4500-5CFA2B(config-smart-cache-policy-test)#
```

```bash
nx4500-5CFA2B(config-smart-cache-policy-test)#show context smart-cache-policy test
  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>Resets or removes cache management settings</td>
</tr>
</tbody>
</table>
4.1.72.2.4 forward-proxy

smart-cache-policy-mode commands

Enables or disables 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, NX6500, NX6524, 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> | Optional. Configures the IP address and TCP port for forward proxying
  | port <1-32768> | This is the IP address where the forward smart caching proxy server is listening.
  | | The default port is 1.

- forward-proxy {protocol [all|ftp|gopher|https]}

  | 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

- forward-proxy {vlan <VLAN-ID>}

  | 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.
  | | • <VLAN-ID> – Specify the list of VLANs.

Examples

nx4500-5CFA2B(config-smart-cache-policy-test)#forward-proxy vlan 10-20
nx4500-5CFA2B(config-smart-cache-policy-test)#

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><code>no</code></td>
<td>Reverts address and port for forward caching proxy service</td>
</tr>
</tbody>
</table>
4.1.72.2.5 http-access

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, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

```
http-access precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|destination-domain-regex <WORD>|destination-ip <IP>|mimetype-regex <WORD>|source-ip <IP>|url-regex <URL>}
```

Parameters

- `http-access precedence <1-100> [deny|permit] {destination-domain <DOMAIN-NAME>|destination-domain-regex <WORD>|destination-ip <IP>|mimetype-regex <WORD>|source-ip <IP>|url-regex <URL>}`

  - `http-access precedence <1-100>` Configures HTTP access rules that determine if a IP address is to be accessed or not. You can create multiple HTTP access rules and assign precedence values to each. These rules are applied in order of their precedence.
    - `<1-100>` – Specify a precedence rule from 1 - 100.
    - **Note:** Lower the precedence, higher is the rule priority.
  - `[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
  - `destination-domain-regex <WORD>` Optional. Specifies a regular expression matching on originating server names
    - 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
    - **Note:** Provide the IP address in the A.B.C.D/M format.
    - **Note:** Specify any to consider all originating servers.
  - `mimetype-regex <WORD>` Optional. Specifies the regular expression used to match the mimetype of a HTTP request
  - `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.
    - **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 originating server hostname
Examples

```
nx4500-5CFA2B(config-smart-cache-policy-test)#http-access precedence 4 deny destination-domain .TechPubs
nx4500-5CFA2B(config-smart-cache-policy-test)#
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
nx4500-5CFA2B(config-smart-cache-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 ACL</td>
</tr>
</tbody>
</table>
4.1.72.2.6 no

- **smart-cache-policy-mode commands**

Removes or resets smart cache policy settings

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [access-log|aging|cache|forward-proxy|http-access|parent-proxy|pre-fetch|smart-cache|transparent-proxy]

**Parameters**

- no [access-log|aging|cache|forward-proxy|http-access|parent-proxy|pre-fetch|smart-cache|transparent-proxy]

- **no access-log** Disables logging of all client requests
- **no aging** Removes the refresh pattern configured with this smart cache policy
- **no cache** Removes cache management settings
- **no forward-proxy** Removes the forward proxy settings
- **no http-access** Removes the ACL associated with this smart cache policy
- **no parent-proxy** Removes the parent proxy settings
- **no pre-fetch** Disables pre-fetching of a URL
- **no smart-cache** Disables smart content caching
- **no transparent-proxy** Removes the transparent proxy settings

**Examples**

The following example displays the content cache policy ‘test’ settings before the no commands are executed:

```plaintext
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

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:

```plaintext
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)#
```
4.1.72.2.7 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, NX6500, NX6524, 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.
| schedule <TIME> | Pre-fetches the specified URL list at a specified time

Examples

nx4500-5CFA2B(config-content-cache-policy-test)#pre-fetch test schedule 12:30
nx4500-5CFA2B(config-content-cache-policy-test)#

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-domain-regex 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 |
4.1.72.2.8 parent-proxy

smart-cache-policy-mode commands

Enables or disables 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, NX6500, NX6524, 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>
<tbody>
<tr>
<td>host &lt;IP/HOST-NAME&gt; port &lt;1-32768&gt;</td>
<td>Configures the hostname or IP address of the parent proxy server</td>
</tr>
</tbody>
</table>

- <IP/HOST-NAME> – Specify the parent proxy server’s IP address or hostname.
- port <> – 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)#

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

nx4500-5CFA2B(config-smart-cache-policy-test)#

Related Commands

no Disables parent proxy on this smart cache policy
4.1.72.2.9 smart-cache

- smart-cache-policy-mode commands

Enables smart content caching

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524, 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 |
4.1.72.2.10 transparent-proxy

smart-cache-policy-mode commands

Enables or disables 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, NX6500, NX6524, 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}}
  - 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>}
  - 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)#

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

nx4500-5CFA2B(config-smart-cache-policy-test)#

Related Commands

no | Resets or removes transparent caching proxy settings
4.1.73 url-list

Global Configuration Commands

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. 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:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

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:
  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.company.com depth 10
nx4500-5CFA2B(config-url-list-URLlist1)#
nx4500-5CFA2B(config-url-list-test)#show context
url-list test
  url http://www.company.com depth 10
nx4500-5CFA2B(config-url-list-URLlist1)#
```
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

Table 5.1 summarizes commands common to the User Exec, Priv Exec, and Global Config modes.

**Table 5.1 Commands Common to Controller CLI 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 5-10</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 (config-if) instance configurations</td>
<td>page 5-13</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system information</td>
<td>page 5-46</td>
</tr>
<tr>
<td>write</td>
<td>Writes the system's running configuration to memory or terminal</td>
<td>page 5-48</td>
</tr>
</tbody>
</table>
5.1.1 clrscr

Common Commands

Clears the screen and refreshes the prompt, irrespective of the mode

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
clrscr

Parameters
None

Examples
The terminal window or screen before the clrscr command is executed:

```plaintext
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
    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:

```plaintext
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
commit {write}{memory}
```

Parameters

- `commit {write}{memory}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write</td>
<td>Optional. If a commit succeeds, the configuration is written to memory</td>
</tr>
<tr>
<td>memory</td>
<td>Optional. Writes to memory</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 will prompt you to either do a commit or a revert before terminating the session.

Supported in the following platforms:
- Access Points — AP300, 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, 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

### Syntax

```
help {search|show}
help {show configuration-tree}
help {search <WORD>} {detailed|only-show|skip-no|skip-show}
```

### Parameters

- **help {show configuration-tree}**

| show configuration-tree | Optional. Displays the running system information
| --- | ---
| configuration-tree | Displays relationship amongst configuration objects

- **help {search <WORD>} {detailed|only-show|skip-no|skip-show}**

| search <WORD> | Optional. Searches for CLI commands related to a specified target term
| --- | ---
| <WORD> | 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.

| detailed | Optional. Searches and displays help strings in addition to mode and commands
| only-show | Optional. Displays only "show" commands. Does not display configuration commands
| skip-no | Optional. Displays only configuration commands. Does not display "no" commands
| skip-show | Optional. Displays only configuration commands. Does not display "show" commands

---

**NOTE:** The `show configuration-tree` option is not available in the Global Config mode.
Examples
rfs7000-37FABE>help search crypto detailed
Found 29 references for “crypto”
Found 113 references for “crypto”
Mode : User Exec
Command : show crypto key rsa (\public-key-detail) (\on DEVICE-NAME))
\ Show running system information
\ Encryption related commands
\ Key management operations
\ Show RSA public Keys
\ Show the public key in PEM format
\ On AP/Controller
\ AP / Controller name

: show crypto pki trustpoints (WORD|all|)\on DEVICE-NAME))
\ Show running system information
\ Encryption related commands
\ Public Key Infrastructure related commands
\ Display the configured trustpoints
\ Display a particular trustpoint's details
\ Display details for all trustpoints
\ On AP/Controller
\ AP / Controller name

: show crypto isakmp sa (\on DEVICE-NAME))
\ Show running system information
\ Encryption Module
\ Show ISAKMP related statistics
\ Show all ISAKMP Security Associations
\ On AP/Controller
\ AP / Controller name

: show crypto ipsec sa (\on DEVICE-NAME))
\ Show running system information
\ Encryption Module
\ Show IPSec related statistics
\ IPSec security association
\ On AP/Controller
\ AP / Controller name

: crypto key generate rsa WORD <1024-2048> \on DEVICE-NAME))
\ Encryption related commands
\ Key management operations
\ Generate a keypair
\ Generate a RSA keypair
\ Keypair name

rfs7000-37FABE>
rfs7000-37FABE>help show configuration-tree
## ACCESS-POINT / SWITCH ## ---+
| +--> [[ RF-DOMAIN ]]
| | +--> [[ PROFILE ]]
| | +--> Device specific parameters (license, serial number, hostname)
| +--> Configuration Overrides of rf-domain and profile
## RF-DOMAIN ## ---+
| +--> RF parameters, WIPS server parameters
| | +--> [[ SMART-RF-POLICY ]]
| +--> [[ WIPS POLICY ]]
## PROFILE ## ---+
| +--> Physical interface (interface GE,ME,UP etc)
| | +--> [[ RATE-LIMIT-TRUST-POLICY ]]
| +--> Vlan interface (interface VLAN1/VLAN36 etc)
| +--> Radio interface (interface RADIO1, RADIO2 etc)
| | +--> Radio specific Configuration
| | +--> [[ RADIO-QOS-POLICY ]]
| | +--> [[ ASSOC-ACL-POLICY ]]
| | +--> [[ WLAN ]]
| +--> [[ MANAGEMENT-POLICY ]]
| +--> [[ DHCP-SERVER-POLICY ]]
| +--> [[ FIREWALL-POLICY ]]
| +--> [[ NAT-POLICY ]]

rfs7000-37FABE>

rfs7000-37FABE>help search clrscr only-show
found no commands containing "clrscr"
rfs7000-37FABE>
COMMON COMMANDS 5-9

rfs7000-37FABE>help search service skip-show
Found 32 references for "service"

Mode : User Exec
Command : service show cli
    : service show rim config (|include-factory)
    : service show wireless credential-cache
    : service show wireless neighbors
    : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
    : service show process(|(on DEVICE-OR-DOMAIN-NAME))
    : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
    : service show top(|(on DEVICE-OR-DOMAIN-NAME))
    : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))
    : service cli-tables-skin (none|minimal|thin|stars|hashes|percent|ansi|utf-8) (grid)
    : service cli-tables-expand (left|right)
    : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
    : service wireless qos delete-tspec AA-BB-CC-DD-EE-FF tid <0-7>
    : service wireless wips clear-event-history
    : service wireless wips clear-mu-blacklist (all|(mac AA-BB-CC-DD-EE-FF))
    : service radio <1-3> dfs simulate-radar (primary|extension)
    : service smart-rf run-calibration
    : service smart-rf stop-calibration
    : service cluster manual-revert
    : service start-shell
    : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio (all|<1-3>)
      (promiscuous)|rim|interface `WORD ge <1-4> me1|pc <1-4> vlan <1-4094>`) (|direction
      (any|inbound|outbound)|acl-name WORD|verbose|hex|count <1-1000000>|snap <1-2048>|write
      (FILE|URL|tzsp WORD|tcpdump})(|filter LINE)

Mode : Profile Mode
Command : service watchdog

Mode : Radio Mode
Command : service antenna-type (default|dual-band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|AP650-int)
    : service disable-erp
    : service disable-ht-protection
    : service recalibration-interval <0-65535>

rfs7000-37FABE>

rfs7000-37FABE>help search mint only-show
Found 8 references for "mint"

Mode : User Exec
Command : show mint neighbors (|details)(|(on DEVICE-NAME))
    : show mint links (|details)(|(on DEVICE-NAME))
    : show mint id(|(on DEVICE-NAME))
    : show mint stats(|(on DEVICE-NAME))
    : show mint route(|(on DEVICE-NAME))
    : show mint lsp
    : show mint lsp-db (|details)(|(on DEVICE-NAME))
    : show mint mlcp(|(on DEVICE-NAME))

rfs7000-37FABE>
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 — AP300, 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, NX5624, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no <PARAMETER>
```

**Parameters**

None

**Usage Guidelines**

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

**Examples**

Global Config mode: No command options
Enter configuration commands, one per line.  End with CNTL/Z.
```
rfs7000-37FABE(config)#no ?
aaa-policy                  Delete a aaa policy
aaa-tacacs-policy           Delete a aaa tacacs policy
alias                       Alias
ap300                       Delete an AP300
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
ap7502                      Delete an AP7502 access point
ap7522                      Delete an AP7522 access point
ap7532                      Delete an AP7532 access point
ap71xx                      Delete an AP71XX access point
ap81xx                      Delete an AP81XX access point
ap82xx                      Delete an AP82XX access point
association-acl-policy      Delete an association-acl policy
auto-provisioning-policy    Delete an auto-provisioning policy
captive-portal             Delete a captive portal
client-identity             Client identity (DHCP Device Fingerprinting)
client-identity-group      Client identity group (DHCP Fingerprint Database)
customize                  Restore the custom cli commands to default
device                     Delete multiple devices
device-categorization      Delete device categorization object
dhcp-server-policy         DHCP server policy
dns-whitelist              Delete a whitelist object
event-system-policy       Delete an event system policy
firewall-policy             Configure 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)
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
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
role-policy                Role based firewall policy
routing-policy             Policy Based Routing Configuration
smart-rf-policy            Delete a smart-rf-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
rfs7000-37FABE(config)#
Priv Exec mode: No command options
rfs7000-37FABE#no ?
adoption                  Reset adoption state of the device (& all devices adopted to it)
captive-portal            Captive portal commands
crypto                    Encryption related commands
debug                     Debugging functions
logging                   Modify message logging facilities
page                      Toggle paging
service                   Service Commands
terminal                  Set terminal line parameters
upgrade                   Remove a patch
wireless                  Wireless Configuration/Statistics commands
rfs7000-37FABE#
user Exec mode: No command options
rfs7000-37FABEx no ?
adoption                  Reset adoption state of the device (& all devices adopted to it)
captive-portal            Captive portal commands
crypto                    Encryption related commands
debug                     Debugging functions
logging                   Modify message logging facilities
page                      Toggle paging
service                   Service Commands
terminal                  Set terminal line parameters
wireless                  Wireless Configuration/Statistics commands
rfs7000-37FABE>

Related Commands

<table>
<thead>
<tr>
<th></th>
<th>User Exec Commands mode</th>
</tr>
</thead>
<tbody>
<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 — AP300, 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, 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax (User Exec Mode)**


service ap300 [dns-name|dot1x|locator|reload]

service ap300 dns-name <DNS-NAME> on [all|ap-mac <MAC>]

service ap300 dot1x username <USERNAME> password <PASSWORD> on [all|ap-mac <MAC>]

service ap300 [locator|reload] <MAC>

service [block-adopter-config-update|request-full-config-from-adopter]

service clear [adoption|captive-portal-page-upload|command-history|device-upgrade|noc|reboot-history|unsanctioned|upgrade-history|virtual-machine-history|wireless|xpath]

service clear adoption history {on <DEVICE-NAME>}

service clear device-upgrade 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 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>}}

{<MAC/hostname>} {<1-3>}

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 enable [l2tpv3|radiusd]
service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}

service force-update-vm-stats {on <DEVICE-NAME>}

service load-balancing clear-client-capability [<MAC]|[all] {on <DEVICE-NAME>}

service locator {<1-60>} {(on <DEVICE-NAME>)}

service radio <1-3> [adaptivity|channel-switch|dfs]

service radio <1-3> channel-switch <36-196> [160|20|40|80|80-80]

service radius test [ <IP>|<HOSTNAME> ] [ <WORD>|<PORT> ]

service radius test [ <IP>|<HOSTNAME> ] <WORD> <USERNAME> { wlan <WLAN-NAME> ssid <SSID> } { on <DEVICE-NAME> }

service show [ block-adopter-config-update|captive-portal|cli|command-history|configuration-revision|crash-info|dhcp-lease|diag|fast-switching|fib|
hardware-switch|info|mac-vendor|mem|mint|noc|pm|process|reboot-history|
rf-domain-manager|sites|snmp|startup-log|sysinfo|top|upgrade-history|
virtual-machine-history|watchdog|wireless|xpath-history]

service show block-adopter-config-update

service show captive-portal [ servers|user-cache ] { on <DEVICE-NAME> }

service show [ cli|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|sysinfo|top|upgrade-history|watchdog ] { on <DEVICE-NAME> }

service show dhcp-lease [ <INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan <1-4094>]

service show diag [ led-status|stats ] { on <DEVICE-NAME> }

service show fast-switching { on <DEVICE-NAME> }

service show fib { table-id <0-255> }

service show hardware-switch mac-address-table

service show mint [ adopted-devices { on <DEVICE-NAME> } | ports ]

service show pm { history } { on <DEVICE-NAME> }

service show rf-domain-manager diag { <MAC/HOSTNAME> } { on <DEVICE-OR-DOMAIN-NAME> }

service show sites

service show virtual-machine-history { on <DEVICE-NAME> }

service show wireless [ aaa-stats|adaptivity-status|ap300|client|config-
internal|credential-cache|dns-cache|log-internal|meshpoint|neighbors|reference|
stats-client|vlan-usage]

service show wireless [ aaa-stats|credential-cache|dns-cache|vlan-usage]

{ on <DEVICE-NAME> }

service show wireless [ ap300 <MAC>|config-internal|log-internal|neighbors]

{ on <DEVICE-OR-DOMAIN-NAME> }

service show wireless [ client|meshpoint neighbor ] proc [ info|stats ] { <MAC> }

{ on <DEVICE-OR-DOMAIN-NAME> }

service show wireless reference dot11 [ frame|handshake|mcs-rates|reason-codes|
status-codes]

service show wireless reference dot11 handshake [ wpa-wpa2-enterprise|
wpa-wpa2-personal]

service show wireless stats-client diag { <MAC/HOSTNAME> } { on <DEVICE-OR-DOMAIN-
NAME> }

service smart-rf [ clear-config|clear-history|interactive-calibration|
interactive-calibration-result|run-calibration|save-config|stop-calibration]

service smart-rf clear-config { <MAC>|<DEVICE-NAME> | on <DOMAIN-NAME> }

service smart-rf [ clear-history|interactive-calibration|run-calibration|save-config|
stop-calibration ] { on <DOMAIN-NAME> }

service smart-rf interactive-calibration-result [ discard|replace-current-config|
write-to-configuration ] { on <DOMAIN-NAME> }
service ssm [dump-core-snapshot|trace]
service ssm trace pattern <WORD> {on <DEVICE-NAME>}

service wireless [client|dump-core-snapshot|meshpoint|qos|trace|wips]
service wireless client [beacon-request|quiet-element|trigger-bss-transition]

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> url <URL> {on <DEVICE-OR-DOMAIN-NAME>

service wireless dump-core-snapshot

service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>

service wireless qos delete-tspec <MAC> tid 0-7

service wireless trace pattern <WORD> {on <DEVICE-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 ap300 dns-name <DNS-NAME> on [all|ap-mac <MAC>]

<table>
<thead>
<tr>
<th>ap300</th>
<th>Configures global AP300 settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-name &lt;DNS-NAME&gt;</td>
<td>Authenticates DNS server name for AP adoption</td>
</tr>
<tr>
<td>on [all</td>
<td>ap-mac &lt;MAC&gt;]</td>
</tr>
</tbody>
</table>

- service ap300 dot1x username <USERNAME> password <PASSWORD> on [all|ap-mac <MAC>]

<table>
<thead>
<tr>
<th>ap300</th>
<th>Configures global AP300 settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>Sets 802.1x authentication parameters</td>
</tr>
<tr>
<td>username &lt;USERNAME&gt;</td>
<td>Authenticates user before providing access</td>
</tr>
<tr>
<td>password &lt;PASSWORD&gt;</td>
<td>Authenticates password before providing access</td>
</tr>
</tbody>
</table>

on [all|ap-mac <MAC>]      | Configures global AP300 parameters on a specified AP300 or all AP300s |

<table>
<thead>
<tr>
<th>ap300</th>
<th>Configures global AP300 settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: This command is not applicable to the NX45XX, NX65XX, and NX9000 series service platforms.</td>
<td></td>
</tr>
<tr>
<td>Note: This command is not applicable to the NX45XX, NX65XX, and NX9000 series service platforms.</td>
<td></td>
</tr>
</tbody>
</table>

<MAC> – Specify the AP300’s MAC address.
- **service ap300 [locator|reload] <MAC>**

  *ap300* Configures global AP300 settings
  
  _Note:_ This command is not applicable to the NX45XX, NX65XX, and NX9000 series service platforms.

  *locator* Enables a specified AP300's LEDs

  *reload* Resets a specified AP300

  *<MAC>* The following keyword is common to 'locator' and 'reload' parameters:
  
  Specifies the AP300's MAC address to enable its locator or to reset the device
  
  - *<MAC>* – Specify the AP300's MAC address.

- **service [block-adopter-config-update|request-full-config-from-adopter]**

  *block-adopter-config-update* Blocks the configuration updates sent from the NOC server

  *request-full-config-from-adopter* Configures a request for full configuration updates from the adopter device

  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 {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 {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 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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`service clear [command-history</td>
<td>reboot-history</td>
</tr>
<tr>
<td>`clear [command-history</td>
<td>reboot-history</td>
</tr>
<tr>
<td><strong>Note</strong>: This command is applicable only on the NX45XX, NX65XX, NX9500, and NX9510 series service platforms.</td>
<td></td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Clears history 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>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: When executing the clear virtual-machine-history command, provide the name of the service platform running the VMs.</td>
<td></td>
</tr>
<tr>
<td><code>clear noc statistics</code></td>
<td>Clears Network Operations Center (NOC) applicable statistics counters</td>
</tr>
<tr>
<td><code>clear unsanctioned aps {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</code></td>
<td>Clears the unsanctioned APs list</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>Optional. Clears the unsanctioned APs list on a specified device or RF Domain.</td>
</tr>
<tr>
<td><strong>&lt;DEVICE-OR-DOMAIN-NAME&gt;</strong> – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
<td></td>
</tr>
<tr>
<td>`clear wireless [ap</td>
<td>client] {&lt;MAC&gt;} {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}`</td>
</tr>
<tr>
<td><strong>ap statistics</strong> – Clears applicable AP statistics counters</td>
<td></td>
</tr>
<tr>
<td><strong>client statistics</strong> – Clears applicable wireless client statistics counters</td>
<td></td>
</tr>
<tr>
<td><strong>&lt;MAC&gt;</strong> {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>The following keywords are common to the ‘ap’ and ‘client’ parameters:</td>
</tr>
<tr>
<td><strong>&lt;MAC&gt;</strong> – Optional. Clears statistics counters for a specified AP or client. Specify the AP/client MAC address.</td>
<td></td>
</tr>
<tr>
<td><strong>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</strong> – 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.</td>
<td></td>
</tr>
<tr>
<td><code>clear wireless controller-mobility-database</code></td>
<td>Clears the controller assisted mobility database</td>
</tr>
<tr>
<td><code>clear wireless radio statistics {&lt;MAC/HOSTNAME&gt;} {&lt;1-3&gt;}</code></td>
<td>Clears applicable wireless radio statistics counters</td>
</tr>
<tr>
<td><strong>&lt;MAC/HOSTNAME&gt;</strong> {&lt;1-3&gt;}</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>service clear wireless wlan statistics <code>{&lt;WLAN-NAME&gt;}</code> <code>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</code></td>
<td>Clears WLAN statistics counters on a specified WLAN and device or RF Domain.</td>
</tr>
<tr>
<td>clear wireless wlan statistics</td>
<td>Clears WLAN statistics counters.</td>
</tr>
<tr>
<td>&lt;WLAN-NAME&gt;</td>
<td>Optional. Clears statistics counters on a specified WLAN. Specify the WLAN name.</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>service clear xpath requests <code>{&lt;1-100000&gt;}</code></td>
<td>Clears XPATH related information and pending XPATH get requests.</td>
</tr>
<tr>
<td>clear xpath</td>
<td>Clears XPATH related information.</td>
</tr>
<tr>
<td>requests</td>
<td>Clears pending XPATH get requests.</td>
</tr>
<tr>
<td>&lt;1-100000&gt;</td>
<td>Optional. Specifies the session number (cookie from show sessions).</td>
</tr>
<tr>
<td>Note:</td>
<td>Omits for this session.</td>
</tr>
<tr>
<td>service cli-tables-skin [ansi</td>
<td>hashes</td>
</tr>
<tr>
<td>cli-tables-skin</td>
<td>Selects a formatting layout or skin for CLI tabular outputs.</td>
</tr>
<tr>
<td>[ansi</td>
<td>hashes</td>
</tr>
<tr>
<td>grid</td>
<td>Optional. Uses a complete grid instead of just title lines.</td>
</tr>
<tr>
<td>service cluster force [active</td>
<td>configured-state</td>
</tr>
<tr>
<td>cluster</td>
<td>Enables cluster protocol management.</td>
</tr>
<tr>
<td>force</td>
<td>Forces action commands on a cluster (active, configured-state, and standby).</td>
</tr>
<tr>
<td>active</td>
<td>Changes the cluster run status to active.</td>
</tr>
<tr>
<td>configured-state</td>
<td>Restores a cluster to the configured state.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>standby</td>
<td>Changes the cluster run status to standby</td>
</tr>
<tr>
<td>• service delete-offline-aps all</td>
<td>Deletes all off-line access points</td>
</tr>
<tr>
<td>delete-offline-aps all</td>
<td>Deletes all off-line access points</td>
</tr>
<tr>
<td>• service delete-offline-aps offline-for days &lt;0-999&gt; {time &lt;TIME&gt;}</td>
<td>Deletes off-line access points for a specified interval</td>
</tr>
<tr>
<td>delete-offline-aps</td>
<td>Deletes off-line access points for a specified interval</td>
</tr>
<tr>
<td>day &lt;0-999&gt;</td>
<td>Deletes off-line access points for a specified number of days</td>
</tr>
<tr>
<td>• &lt;0-999&gt; – Specify the number of off-line days from 0 - 999.</td>
<td></td>
</tr>
<tr>
<td>time &lt;TIME&gt;</td>
<td>Optional. Deletes off-line access points for a specified time</td>
</tr>
<tr>
<td>• &lt;TIME&gt; – Specify the time in HH:MM:SS format.</td>
<td></td>
</tr>
<tr>
<td>• service enable [l2tpv3</td>
<td>radiusd]</td>
</tr>
<tr>
<td>enable l2tpv3</td>
<td>Enables L2TPv3 on low memory devices</td>
</tr>
<tr>
<td>enable radiusd</td>
<td>Enables RADIUS server loading on low memory devices</td>
</tr>
<tr>
<td>• service force-send-config {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
<td>Resends configuration to device(s)</td>
</tr>
<tr>
<td>force-send-config</td>
<td>Resends configuration to device(s)</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Resends configuration to a specified device or all devices in a specified 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>• service force-update-vm-stats {on &lt;DEVICE-NAME&gt;}</td>
<td>Forcefully pushes VM statistics on to the NOC</td>
</tr>
<tr>
<td>force-update-vm-stats</td>
<td>Forcefully pushes VM statistics on to the NOC</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Executes the command on a specified device</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the device.</td>
<td></td>
</tr>
<tr>
<td>• service load-balancing clear-client-capability [&lt;MAC&gt;</td>
<td>all] {on &lt;DEVICE-NAME&gt;}</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Enables wireless load balancing by clearing client capability records</td>
</tr>
<tr>
<td>clear-client-capability [&lt;MAC&gt;</td>
<td>all]</td>
</tr>
<tr>
<td>• &lt;MAC&gt; – Clears capability records of a specified client. Specify the client’s MAC address in the AA-BB-CC-DD-EE-FF format.</td>
<td></td>
</tr>
<tr>
<td>• all – Clears the capability records of all clients</td>
<td></td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Clears client capability records on a specified device</td>
</tr>
<tr>
<td>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
<tr>
<td>• service locator {&lt;1-60&gt;} {on &lt;DEVICE-NAME&gt;}</td>
<td>Enables LEDs</td>
</tr>
<tr>
<td>locator</td>
<td>Enables LEDs</td>
</tr>
<tr>
<td>&lt;1-60&gt;</td>
<td>Sets LED flashing time from 1 - 60 seconds.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>service radio &lt;1-3&gt; &lt;adaptivity</td>
<td>channel-switch &lt;36-196&gt; [160</td>
</tr>
<tr>
<td>adaptivity</td>
<td>Simulates adaptivity on a given radio channel</td>
</tr>
<tr>
<td>channel-switch &lt;36-196&gt; [160</td>
<td>20</td>
</tr>
<tr>
<td>radio &lt;1-3&gt;</td>
<td>Configures radio’s parameters</td>
</tr>
<tr>
<td>dfs</td>
<td>Enables Dynamic Frequency Selection (DFS)</td>
</tr>
<tr>
<td>simulate-radar [extension</td>
<td>primary]</td>
</tr>
<tr>
<td>service radius test [&lt;IP&gt;</td>
<td>&lt;HOSTNAME&gt;] &lt;WORD&gt; &lt;USERNAME&gt; &lt;PASSWORD&gt; {wlan &lt;WLAN-NAME&gt; ssid &lt;SSID&gt;}</td>
</tr>
<tr>
<td>radius test</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>&lt;HOSTNAME&gt;</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>Specify the RADIUS server’s shared secret.</td>
</tr>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify username for authentication.</td>
</tr>
<tr>
<td>&lt;PASSWORD&gt;</td>
<td>Specify the password.</td>
</tr>
<tr>
<td>wlan &lt;WLAN-NAME&gt; ssid &lt;SSID&gt;</td>
<td>Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device</td>
</tr>
</tbody>
</table>

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 radius test** [<IP>|<HOSTNAME>] <PORT> <1024-65535> <WORD> <USERNAME> <PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius test</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>[&lt;IP&gt;</td>
<td>&lt;HOSTNAME&gt;]</td>
</tr>
<tr>
<td>&lt;PORT&gt;</td>
<td>Specify the RADIUS server's IP address.</td>
</tr>
<tr>
<td>&lt;1024-65535&gt;</td>
<td>Specify the RADIUS server port from 1024 - 65535. The default port is 1812.</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>Specify the RADIUS server's shared secret.</td>
</tr>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify username for authentication.</td>
</tr>
<tr>
<td>&lt;PASSWORD&gt;</td>
<td>Specify the password.</td>
</tr>
<tr>
<td>wlan &lt;WLAN-NAME&gt; ssid &lt;SSID&gt;</td>
<td>Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device</td>
</tr>
</tbody>
</table>

- **service set validation-mode** [full|partial] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the validation mode for running configuration validation</td>
</tr>
<tr>
<td>validation-mode [full</td>
<td>partial]</td>
</tr>
<tr>
<td>full</td>
<td>Performs a full configuration validation</td>
</tr>
<tr>
<td>partial</td>
<td>Performs a partial configuration validation</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Performs full or partial configuration validation on a specified device</td>
</tr>
</tbody>
</table>

- **service show block-adopter-config-update**

<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>block-adopter-config-update</td>
<td>Displays NOC configuration blocking status</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>Service</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show</code></td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td><code>cli</code></td>
<td>Displays CLI tree of the current mode</td>
</tr>
<tr>
<td><code>configuration-revision</code></td>
<td>Displays current configuration revision number</td>
</tr>
<tr>
<td><code>mac-vendor &lt;OUI/MAC&gt;</code></td>
<td>Displays vendor name for a specified MAC address or Organizationally Unique Identifier (OUI) part of the MAC address</td>
</tr>
<tr>
<td><code>noc diag</code></td>
<td>Displays NOC diagnostic details</td>
</tr>
<tr>
<td><code>snmp session</code></td>
<td>Displays SNMP session details</td>
</tr>
<tr>
<td><code>xpath-history</code></td>
<td>Displays XPath history</td>
</tr>
<tr>
<td><code>command-history</code></td>
<td>Displays command history (lists all commands executed)</td>
</tr>
<tr>
<td><code>crash-info</code></td>
<td>Displays information about core, panic, and AP dump files</td>
</tr>
<tr>
<td><code>info</code></td>
<td>Displays snapshot of available support information</td>
</tr>
<tr>
<td><code>mem</code></td>
<td>Displays a system’s current memory usage (displays the total memory and available memory)</td>
</tr>
<tr>
<td><code>process</code></td>
<td>Displays active system process information (displays all processes currently running on the system)</td>
</tr>
<tr>
<td><code>reboot-history</code></td>
<td>Displays the device’s reboot history</td>
</tr>
<tr>
<td><code>startup-log</code></td>
<td>Displays the device’s startup log</td>
</tr>
<tr>
<td><code>sysinfo</code></td>
<td>Displays system’s memory usage information</td>
</tr>
<tr>
<td><code>top</code></td>
<td>Displays system resource information</td>
</tr>
<tr>
<td><code>upgrade-history</code></td>
<td>Displays the device’s upgrade history (displays details, such as date, time, and status of the upgrade, old version, new version etc.)</td>
</tr>
<tr>
<td><code>watchdog</code></td>
<td>Displays the device’s watchdog status</td>
</tr>
</tbody>
</table>

The following keywords are common to all of the above:
- `on <DEVICE-NAME>` – Optional. Displays information for a specified device. If no device is specified, the system displays information for logged device(s)
- `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.
**service show dhcp-lease**

<table>
<thead>
<tr>
<th>show dhcp-lease</th>
<th>Displays running system statistics based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;INTERFACE&gt;</code></td>
<td>Optional. Displays DHCP lease information for a specified router interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;INTERFACE&gt;</code> – Specify the router interface name.</td>
</tr>
<tr>
<td><code>on</code></td>
<td>Optional. Displays DHCP lease information for a specified device</td>
</tr>
<tr>
<td><code>pppoe1</code></td>
<td>Optional. Displays DHCP lease information for a PPP over Ethernet interface</td>
</tr>
<tr>
<td><code>vlan &lt;1-4094&gt;</code></td>
<td>Optional. Displays DHCP lease information for a VLAN interface</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-4094&gt;</code> – Specify a VLAN index from 1 - 4094.</td>
</tr>
<tr>
<td><code>wwan1</code></td>
<td>Optional. Displays DHCP lease information for a Wireless WAN interface</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>The following keywords are common to all of the above:</td>
</tr>
<tr>
<td></td>
<td>• <code>on &lt;DEVICE-NAME&gt;</code> – 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>• <code>&lt;DEVICE-NAME&gt;</code> – Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

**service show diag**

| show diag [led-status|stats] | Displays running system statistics based on the parameters passed |
|---------------------|---------------------------------------------------------------|
| `diag`              | Displays diagnostic statistics, such as LED status, fan speed, and sensor temperature |
| `led-status`        | Displays LED state variables and the current state |
| `stats`             | Displays fan speed and sensor temperature statistics |
| `on <DEVICE-NAME>`  | Optional. Displays diagnostic statistics 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. |

**service show fast-switching**

<table>
<thead>
<tr>
<th>show fast-switching</th>
<th>Displays running system statistics based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fast-switching</code></td>
<td>Displays fast switching state</td>
</tr>
<tr>
<td><code>on &lt;DEVICE-NAME&gt;</code></td>
<td>Optional. Displays fast switching state for a specified device. If no device is specified, the system displays information for the logged 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>

**service show fib**

<table>
<thead>
<tr>
<th>show fib {table-id &lt;0-255&gt;}</th>
<th>Displays running system statistics based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>table-id &lt;0-255&gt;</code></td>
<td>Optional. Displays the FIB table for the specified table ID.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>service show hardware-switch mac-address-table</td>
<td>Displays the mac-address-table. Note: This command is available only the NX45XX and NX65XX series service platforms.</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>hardware-switch mac-address-table</td>
<td>Displays the mac-address-table</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>mint</td>
<td>Displays MiNT protocol details</td>
</tr>
<tr>
<td>adopted-devices on &lt;DEVICE-NAME&gt;</td>
<td>Displays adopted devices status in dpd2</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>on &lt;DEVICE-NAME&gt; – Optional. Displays MiNT protocol details for a specified device. If no device is specified, the system displays information for the logged device.</td>
</tr>
<tr>
<td>ports</td>
<td>Displays MiNT ports used by various services and features</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>pm</td>
<td>Displays the Process Monitor (PM) controlled process details</td>
</tr>
<tr>
<td>history</td>
<td>Optional. Displays process change history (the time at which the change was implemented, and the events that triggered the change)</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays process change history for a specified device. If no device is specified, the system displays information for the logged device.</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</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>rf-domain-manager diag &lt;MAC/HOSTNAME&gt; on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Displays RF Domain manager related diagnostics statistics on a specified device or domain</td>
</tr>
<tr>
<td>&lt;MAC/HOSTNAME&gt;</td>
<td>Optional. Specify the MAC address or hostname of the RF Domain manager.</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>sites</td>
<td>Displays NOC sites related information</td>
</tr>
</tbody>
</table>
- **service show virtual-machine-history** 
  
  **show virtual-machine-history** 
  Displays virtual machine history based on the parameters passed  
  **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.  
  
  **on <DEVICE-NAME>** 
  Displays virtual machine history on a specified device. If no device is specified, the system displays information for the logged device.  
  • **<DEVICE-NAME>** — Specify the name of the service platform.  
  
- **service show wireless** 
  
  **show wireless [aaa-stats|adaptivity-status|credential-cache|dns-cache|vlan-usage]**  
  
  **show** 
  Displays running system statistics based on the parameters passed  
  **wireless** 
  Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)  
  **aaa-stats** 
  Displays AAA policy statistics  
  **adaptivity-status** 
  Displays the current list of channels and time when the adaptivity was initiated on a particular device  
  **credential-cache** 
  Displays clients cached credentials statistics (VLAN, keys etc.)  
  **dns-cache** 
  Displays cache of resolved names of servers related to wireless networking  
  **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 [ap300 <MAC>|config-internal|log-internal|neighbors]**  
  
  **show** 
  Displays running system statistics based on the parameters passed  
  **wireless** 
  Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)  
  **ap300 <MAC>** 
  Displays a WLAN’s AP300 statistics  
  • **<MAC>** — Specify the AP300’s MAC address.  
  **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>}** 
  
  **show** 
  Displays running system statistics based on the parameters passed  
  **wireless** 
  Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)
<table>
<thead>
<tr>
<th>Client</th>
<th>Displays WLAN client statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meshpoint neighbor</td>
<td>Displays meshpoint related proc entries</td>
</tr>
</tbody>
</table>
| 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 wireless client or neighbor.  |
| Stats       | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified wireless client or neighbor.  |
| <MAC>       | Displays information for a specified wireless client or neighbor.  |
| On <DEVICE-OR-DOMAIN-NAME> | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified wireless client or neighbor.  |

- `service show wireless reference dot11 [frame|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.

### dot11
- Displays 802.11 standard related information, such as frame structure, MCS rates etc.

### frame
- Displays 802.11 frame structure

### 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 reference dot11 handshake {wpa-wpa2-enterprise/ wpa-wpa2-personal}`

### 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.

### dot11
- Displays 802.11 standard related information, such as frame structure, MCS rates etc.

### handshake
- Displays a flow diagram of 802.11 handshakes

### wpa-wpa2-enterprise
- Optional. Displays a WPA/WPA2 enterprise handshake (TKIP/CCMP with 802.1x authentication)

### wpa-wpa2-personal
- Optional. Displays a WPA/WPA2 personal handshake (TKIP/CCMP with pre-shared keys)
### COMMON COMMANDS

#### service show wireless stats-client diag

<table>
<thead>
<tr>
<th>show</th>
<th>Displays running system statistics based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless</td>
<td>Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)</td>
</tr>
<tr>
<td>stats-client</td>
<td>Displays managed AP statistics</td>
</tr>
<tr>
<td>&lt;MAC/HOSTNAME&gt;</td>
<td>Optional. Specify the MAC address or hostname of the AP.</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Displays statistics on a specified AP, or all APs on a specified domain.</td>
</tr>
</tbody>
</table>

#### service smart-rf clear-config

| smart-rf | Enables Smart RF management |
| clear-config | Clears WLAN Smart RF configuration on a specified device or on all devices |
| <MAC> | 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. |
| <DEVICE-NAME> | Optional. Clears WLAN Smart RF configuration on a device identified by its hostname. Specify the device’s hostname. |
| on <DOMAIN-NAME> | Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain |

#### service smart-rf interactive-calibration

| smart-rf | Enables Smart RF management |
| clear-history | Clears WLAN Smart RF history on all devices |
| interactive-calibration | Enables an interactive Smart RF calibration |
| run-calibration | Starts a new Smart RF calibration process |
| save-config | Saves the Smart RF configuration on all devices, and also saves the history on the RF Domain Manager |
| stop-calibration | Stops an in-progress Smart RF calibration |
| on <DOMAIN-NAME> | Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain |

#### service smart-rf interactive-calibration-result

| smart-rf | Enables Smart RF management |
| interactive-calibration-result | Displays interactive Smart RF calibration results |
| discard | Discards interactive Smart RF calibration results |
| replace-current-config | Replaces current radio configuration |
### Service Debugging Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service ssm dump-core-snapshot</code></td>
<td>Triggers a debug core dump of the SSM module</td>
</tr>
<tr>
<td><code>service ssm trace pattern &lt;WORD&gt; {on &lt;DEVICE-NAME&gt;}</code></td>
<td>Displays the SSM module trace based on parameters passed</td>
</tr>
<tr>
<td>`service wireless client beacon-request &lt;MAC&gt; mode [active</td>
<td>passive</td>
</tr>
</tbody>
</table>
| `wireless client quiet-element [start|stop]`  | Enables/disables the quite-element information in beacons sent to wireless clients
<p>| <code>start</code>                                      | Enables the quite-element information in beacons sent to wireless clients. This is the interval for which all wireless clients are to remain quiet. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>stop</strong></td>
<td>Disables the quiet-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> url <URL> {on <DEVICE-OR-DOMAIN-NAME>} | Sends a 80211v-Wireless Network Management BSS transition request to a client. <MAC> Specifies the wireless client's MAC address. url <URL> 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. |
| **wireless client trigger-bss-transition**        | Sends a 80211v-Wireless Network Management BSS transition request to a client. |
| <MAC>                                            | Specifies the wireless client's MAC address.                                 |
| url <URL>                                        | 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 dump-core-snapshot**         | Triggers a debug core-dump of the wireless module.                          |
| **wireless client dump-core-snapshot**            | Triggers a debug core-dump of the wireless module.                          |
| • **service wireless meshpoint** zl <MESHPOINT-NAME> {on <DEVICE-NAME>} {<ARGS>} | Runs zonal level commands for a meshpoint.  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, service platform, or service platform. |
| **wireless meshpoint**                           | Runs zonal level commands for a meshpoint.                                  |
| **zl**                                           | Runs zonal commands.                                                         |
| <MESHPOINT-NAME>                                 | Runs zonal commands for the meshpoint identified by the <MESHPOINT-NAME> keyword. |
| on <DEVICE-NAME>                                 | Runs zonal commands for the specified meshpoint on a specified AP, wireless controller, or service platform. |
| <ARGS>                                           | Optional. Specifies the zonal arguments.  
  • <ARGS> – Specify the zonal arguments. |
| • **service wireless qos delete-tspec** <MAC> tid <0-7> | Sends a delete TSPEC request to a wireless client.  
  • <MAC> – Specify the MAC address of the wireless client.  
  • tid <0-7> – Select the TID from 0 - 7. |
| **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> – Select the TID from 0 - 7. |
| tid <0-7>                                        | Deletes the Traffic Identifier (TID).  
  • <0-7> – Select the TID from 0 - 7. |
| • **service wireless trace pattern** <WORD> {on <DEVICE-NAME>} | Displays the wireless module trace based on parameters passed.  
  • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. |
| **wireless trace**                               | 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. |
### Wireless WIPS Management

- **service wireless wips clear-client-blacklist [all|mac <MAC>]**

  Enables management of WIPS parameters

  **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>}**

  Enables WIPS management

  **clear-event-history**
  - Clears event history
    - **on <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 parameters sections of this chapter.

**service**

- **service copy tech-support [<FILE>|<URL>]**
- **service clear crash-info {on <DEVICE-NAME>}**
- **service delete sessions <SESSION-COOKIES>**
- **service mint [clear|debug-log|expire|flood]**
- **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 <1-2048>, tcpdump,verbose,write [file|url|tzsp [IP/TZSP-HOSTNAME]])**
- **service pktcap on interface [<INTERFACE-NAME]|ge <1-4>|mel|port-channel <1-2]| pppoe|vlan <1-4094]|wwan1] {acl-name <ACL>,count <1-1000000>, direction [any|inbound|outbound],filter <LINE>,hex,rate <1-100>, snap <1-2048>,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 <1-2048>,tcpdump,verbose,write [file|url|tzsp [IP/TZSP-HOSTNAME]])}
- **service pm stop {on <DEVICE-NAME>}}
- **service show last-passwd**
- **service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]**
- **service start-shell**
- **service syslog test {level [0-7]|alerts|critical|debugging|emergencies|errors| informational|notifications|warnings} {on <DEVICE-NAME>}}
- **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 files for technical support</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FILE&gt;</td>
<td>Specify the file name and location using one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>cf:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb1:/path/file</td>
</tr>
<tr>
<td></td>
<td>usb2:/path/file</td>
</tr>
<tr>
<td>&lt;URL&gt;</td>
<td>Specify the file location in one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>tftp://&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname</td>
</tr>
<tr>
<td></td>
<td>sftp://&lt;user&gt;:&lt;passwd&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>&lt;DEVICE-NAME&gt;</td>
<td>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</th>
<th>Deletes session cookies</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SESSION-COOKIES&gt;</td>
<td>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>
<tbody>
<tr>
<td>clear [lsp-dp</td>
<td>mlcp]</td>
</tr>
<tr>
<td>debug-log [flash-and-syslog</td>
<td>flash-only]</td>
</tr>
<tr>
<td>expire [lsp</td>
<td>spf]</td>
</tr>
<tr>
<td>flood [csnp</td>
<td>lsp]</td>
</tr>
</tbody>
</table>

- <FILE> Specify the file name and location using one of the following formats:
- <URL> Specify the file location in one of the following formats:

- <DEVICE-NAME> Specify the name of the AP, wireless controller, or service platform.
### service pm stop {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>pm</th>
<th>Stops the Process Monitor (PM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>stops</td>
<td>Stops the PM from monitoring all daemons</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Stops the PM 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>

### 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>]}}

<table>
<thead>
<tr>
<th>pktcap on</th>
<th>Captures data packets crossing at a specified location</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>
<tr>
<td>direction [any</td>
<td>inbound</td>
</tr>
<tr>
<td>Filter Options</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>&lt;LINE&gt;</code></td>
<td>Defines user defined packet capture filter</td>
</tr>
<tr>
<td><code>arp</code></td>
<td>Matches ARP packets</td>
</tr>
<tr>
<td><code>capwap</code></td>
<td>Matches CAPWAP packets</td>
</tr>
<tr>
<td><code>cdp</code></td>
<td>Matches CDP packets</td>
</tr>
<tr>
<td><code>dot11</code></td>
<td>Matches 802.11 packets</td>
</tr>
<tr>
<td><code>dropreason</code></td>
<td>Matches packet drop reason</td>
</tr>
<tr>
<td><code>dst</code></td>
<td>Matches IP destination</td>
</tr>
<tr>
<td><code>ether</code></td>
<td>Matches Ethernet packets</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Matches host destination</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Matches ICMP packets</td>
</tr>
<tr>
<td><code>igmp</code></td>
<td>Matches IGMP packets</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Matches IPV4 packets</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>Matches IPV6 packets</td>
</tr>
<tr>
<td><code>l2</code></td>
<td>Matches L2 header</td>
</tr>
<tr>
<td><code>l3</code></td>
<td>Matches L3 header</td>
</tr>
<tr>
<td><code>l4</code></td>
<td>Matches L4 header</td>
</tr>
<tr>
<td><code>lldp</code></td>
<td>Matches LLDP packets</td>
</tr>
<tr>
<td><code>mint</code></td>
<td>Matches MiNT packets</td>
</tr>
<tr>
<td><code>net</code></td>
<td>Matches IP in subnet</td>
</tr>
<tr>
<td><code>not</code></td>
<td>Filters out any packet that matches the filter criteria</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Matches TCP or UDP port</td>
</tr>
<tr>
<td><code>priority</code></td>
<td>Matches packet priority</td>
</tr>
<tr>
<td><code>radio</code></td>
<td>Matches radio</td>
</tr>
<tr>
<td><code>src</code></td>
<td>Matches IP source</td>
</tr>
<tr>
<td><code>stp</code></td>
<td>Matches STP packets</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Matches TCP packets</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Matches UDP packets</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>Matches VLAN</td>
</tr>
<tr>
<td><code>wlan</code></td>
<td>Matches WLAN</td>
</tr>
<tr>
<td>hex</td>
<td>Optional. Provides binary output of the captured packets</td>
</tr>
<tr>
<td>rate <code>&lt;1-100&gt;</code></td>
<td>Optional. Specifies the packet capture rate</td>
</tr>
<tr>
<td>snap <code>&lt;1-2048&gt;</code></td>
<td>Optional. Captures the data length</td>
</tr>
<tr>
<td>tcpdump</td>
<td>Optional. Decodes tcpdump. The tcpdump analyzes network behavior, performance, and infrastructure. It also analyzes applications that generate or receive traffic.</td>
</tr>
</tbody>
</table>
**pktcap on radio**

Captures data packets on a radio (802.11)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1024&gt;</td>
<td>Captures data packets on a specified radio</td>
</tr>
<tr>
<td>all</td>
<td>Captures data packets on all radios</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. Sets a specified number of packets to capture</td>
</tr>
<tr>
<td>direction [any</td>
<td>inbound</td>
</tr>
<tr>
<td>filter &lt;LINE&gt;</td>
<td>Optional. Filters packets based on the option selected (must be used as a last option)</td>
</tr>
<tr>
<td>hex</td>
<td>Optional. Provides binary output of the captured packets</td>
</tr>
<tr>
<td>rate &lt;1-100&gt;</td>
<td>Optional. Specifies the packet capture rate</td>
</tr>
<tr>
<td>snap &lt;1-2048&gt;</td>
<td>Optional. Captures the data length</td>
</tr>
<tr>
<td>tcpdump</td>
<td>Optional. Decodes the TCP dump</td>
</tr>
<tr>
<td>verbose</td>
<td>Optional. Provides verbose output</td>
</tr>
</tbody>
</table>

- **service pktcap on radio**

```
{<acl-name <ACL>, count <1-1000000>, direction [any|inbound|outbound], filter <LINE>, hex, promiscuous, rate <1-100>, snap <1-2048>,
 tcpdump, verbose, write [file|url|tzsp <IP/TZSP-HOSTNAME>])}
```

* optional.
### COMMON COMMANDS

#### write
Captures packets to a specified file. Provide the file name and location in the following format:
- **FILE** – flash:/path/file
  - cf:/path/file
  - usb1:/path/file
  - usb2:/path/file
  - nvram:startup-config
- **URL** – tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
  - sftp://<user>@<hostname|IP>[:port]/path/file
- **tzsp** – The TZSP host. Specify the TZSP host’s IP address or hostname.

### service pktcap on interface
**on** – Specify the capture location.

<table>
<thead>
<tr>
<th><strong>interface</strong></th>
<th>Captures data packets at a specified interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;INTERFACE&gt;</code>, <code>ge &lt;1-4&gt;</code>, <code>port-channel &lt;1-2&gt;</code>, <code>vlan &lt;1-4094&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

- **<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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write</td>
<td>Captures packets to a specified file. Provide the file name and location in the following format: FILE – flash:/path/file cf:/path/file usb1:/path/file usb2:/path/file nvram:startup-config URL – tftp://&lt;hostname</td>
</tr>
<tr>
<td>show</td>
<td>Displays running system statistics based on the parameters passed</td>
</tr>
<tr>
<td>last-passwd</td>
<td>Displays the last password used to enter shell</td>
</tr>
<tr>
<td>signal</td>
<td>Sends a signal to a process</td>
</tr>
<tr>
<td>abort</td>
<td>Sends an abort signal to a process, and forces it to dump to core</td>
</tr>
<tr>
<td>kill</td>
<td>Sends a kill signal to a process, and forces it to terminate without a core</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provides shell access</td>
</tr>
<tr>
<td>syslog test</td>
<td>Sends a test message to the syslog server to confirm server availability</td>
</tr>
<tr>
<td>level</td>
<td>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.</td>
</tr>
</tbody>
</table>

- <0-7> – Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:
  - 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). This is the default setting.
**service trace <PROCESS-NAME>**

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 analytics [clear-data|get-last-detailed-status|migrate|nfsserver|primary|restart|secondary|start|start-detailed-status|status|stop|wifi]
```

```
service analytics nfsserver [<IP>|<HOST-NAME>]
```

```
service analytics primary [<IP>|<HOST-NAME>]
```

```
service analytics secondary [<IP>|<HOST-NAME>]
```

```
service copy [<URL]|analytics-support|mac-user-db|tech-support]
```

```
service copy <URL>
```

```
service copy analytics-support [<FILE>|<URL>]
```

```
service copy mac-user-db <URL>
```

### Parameters (Privilege Exec Mode: NX9000, NX9500, and NX9510)

**service**

- service analytics [clear-data|get-last-detailed-status|migrate|restart|start|start-detailed-status|status|stop|wifi]

**service analytics** Provides analytics services

**Note:** The analytics feature is a separately licensed feature available only on the NX9500 and NX9510 model (NOC) service platforms and their managed controllers, service platforms, and access points. When enabled, this feature provides granular and robust analytic reporting for a controller managed (RFS4000, RFS6000, RFS7000, NX45XX, and NX65XX) network. Using analytics, data is collected at administrator defined intervals.

**Note:** Use nfsserver command to configure the Network File Server (NFS)

**Note:** To configure the license string for the hotspot analytics feature, see license.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear-data</td>
<td>Clears analytics data</td>
</tr>
<tr>
<td>get-last-detailed-status</td>
<td>Retrieves the last detailed status (Hadoop/Hbase status and database sync status)</td>
</tr>
<tr>
<td>migrate</td>
<td>Deletes current analytics data and migrated 5.4.X analytics data</td>
</tr>
<tr>
<td>restart</td>
<td>Restarts analytics services</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>start</td>
<td>Starts analytics services</td>
</tr>
<tr>
<td>start-detailed-status</td>
<td>Initiates a detailed status computation</td>
</tr>
<tr>
<td>status</td>
<td>Displays the status of analytics services</td>
</tr>
<tr>
<td>stop</td>
<td>Stops analytics services</td>
</tr>
<tr>
<td>wifi</td>
<td>Enables WiFi statistics polling. When enabled, this feature processes and stores wireless statistics and events in the Analytics module. This feature is disabled by default.</td>
</tr>
<tr>
<td>Note:</td>
<td>To check WiFi data polling status, execute the <code>service &gt; analytics &gt; status</code> command.</td>
</tr>
<tr>
<td>Note:</td>
<td>To disable WiFi data polling, execute the <code>no &gt; service analytics &gt; wifi</code> command.</td>
</tr>
</tbody>
</table>

- **service analytics nfsserver [<IP>|<HOST-NAME>]**

  Configures the analytics NFS server. Use one of the following options to identify the NFS server:
  - `<IP>` – Specifies the NFS server’s IP address
  - `<HOST-NAME>` – Specifies the NFS server’s hostname

- **service analytics primary [<IP>|<HOST-NAME>]**

  Configures the analytics primary server. Use one of the following options to identify the primary server:
  - `<IP>` – Specifies the primary server’s IP address
  - `<HOST-NAME>` – Specifies the primary server’s hostname

- **service analytics secondary [<IP>|<HOST-NAME>]**

  Configures the analytics secondary server. Use one of the following options to identify the secondary server:
  - `<IP>` – Specifies the secondary server’s IP address
  - `<HOST-NAME>` – Specifies the secondary server’s hostname

- **service copy analytics-support [<FILE>|<URL>]**

  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.

  - `<FILE>` Specify the file name and location using one of the following formats:
    - `usb1:/path/file`
    - `usb2:/path/file`

  - `<URL>` Specify the file location in 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`
- **service copy <URL>**

  Copy command, imports files from a specified location. Use one of the following options to specify the file to copy and the location:

  - URL — tftp://<hostname|IP>:<port>/path/file
  - ftp://<user>:<passwd>@<hostname|IP>:<port>/path/file
  - sftp://<user>@<hostname|IP>:<port>/path/file

- **service copy mac-user-db <URL>**

  Copy command, exports MAC user database file (in the comma-separated values (CSV) format) to a specified location. Use one of the following options to specify the file to copy and the location:

  - URL — tftp://<hostname|IP>:<port>/path/file
  - ftp://<user>:<passwd>@<hostname|IP>:<port>/path/file
  - sftp://<user>@<hostname|IP>:<port>/path/file

**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>}
```

**Parameters (Global Config Mode)**

- **service set [command-history <10-300>|upgrade-history <10-100>|reboot-history <10-100>] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>set</th>
<th>Sets the size of history files</th>
</tr>
</thead>
<tbody>
<tr>
<td>command-history &lt;10-300&gt;</td>
<td>Sets the size of the command history file</td>
</tr>
<tr>
<td></td>
<td>- &lt;10-300&gt; – Specify a value from 10 - 300. The default is 200.</td>
</tr>
<tr>
<td>upgrade-history &lt;10-100&gt;</td>
<td>Sets the size of the upgrade history file</td>
</tr>
<tr>
<td></td>
<td>- &lt;10-100&gt; – Specify a value from 10 - 100. The default is 50.</td>
</tr>
<tr>
<td>reboot-history &lt;10-100&gt;</td>
<td>Sets the size of the reboot history file</td>
</tr>
<tr>
<td></td>
<td>- &lt;10-100&gt; – Specify a value from 10 - 100. The default is 50.</td>
</tr>
</tbody>
</table>
virtual-machine-history <10-200> | Sets the size of the virtual-machine history file
| • <10-200> – Specify a value from 10 - 200. The default is 100.

Note: This command is applicable only to the NX45XX, NX65XX, NX9500, and NX9510 series service platforms. Use the `no > service > set > virtual-machine-history` to revert the history file size to 100.

on <DEVICE-NAME> | Optional. Sets the size of history files on a specified device
| • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

• 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 pktcap on interface vlan 2
Capturing up to 50 packets. Use Ctrl-C to abort.

rfs7000-37FABE>service show cli
User Exec mode: +do
+help [help]
  +do
  +show
    +configuration-tree [help show configuration-tree]
    +search
      +WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
    +show
      +commands [show commands]
      +running-config [show (running-config|session-config) (|include-factory)]
      +-include-factory [show (running-config|session-config) (|include-factory)]
    +interface [show running-config interface (|WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>) (|include-factory)]
      +WORD [show running-config interface (|WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>) (|include-factory)]
      +-include-factory [show running-config interface (|WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>) (|include-factory)]
    +show
      +commands [show commands]
      +interface [show running-config interface (|WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>) (|include-factory)]
      +-include-factory [show running-config interface (|WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>) (|include-factory)]
      +-interface [show running-config interface (|WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>) (|include-factory)]

--More--
rfs7000-37FABE>

rfs7000-37FABE#service signal kill testp
Sending a kill signal to testp
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 Config mode:
  +help [help]
  +search
    +WORD [help search WORD (|detailed|only-show|skip-show)]
```plaintext
++detailed [help search WORD ({detailed|only-show|skip-show})]
++only-show [help search WORD ({detailed|only-show|skip-show})]
++skip-show [help search WORD ({detailed|only-show|skip-show})]
++show
++commands [show commands]
++eval
++LINE [show eval LINE]
++debugging [show debugging ({(on DEVICE-OR-DOMAIN-NAME)})]
++cfgd [show debugging cfgd]
++on
++DEVICE-OR-DOMAIN-NAME [show debugging (({on DEVICE-OR-DOMAIN-NAME}))]
++wireless [show debugging wireless ({(on DEVICE-OR-DOMAIN-NAME)})]
++on
++DEVICE-OR-DOMAIN-NAME [show debugging wireless (({on DEVICE-OR-DOMAIN-NAME}))]
++on
++DEVICE-OR-DOMAIN-NAME [show debugging voice (({on DEVICE-OR-DOMAIN-NAME}))]
--More--
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>Feb 15 14:44:19 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>clock set 14:45:30 15 Feb 2014</td>
</tr>
<tr>
<td>Feb 15 14:41:10 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>clear event-history</td>
</tr>
<tr>
<td>Feb 15 14:38:28 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>boot system primary</td>
</tr>
<tr>
<td>Feb 15 14:35:54 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>boot system secondary</td>
</tr>
<tr>
<td>Jan 31 01:05:58 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload cancel-upload 00-04-96-4A-A7-08</td>
</tr>
<tr>
<td>Jan 31 01:04:45 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload cancel-upload on rf-domain test</td>
</tr>
<tr>
<td>Jan 31 01:02:56 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload cancel-upload on rf-domain default</td>
</tr>
<tr>
<td>Jan 31 01:01:22 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload test1 00-04-96-4A-A7-08 upload-time 03/01/2014-12:30</td>
</tr>
<tr>
<td>Jan 31 01:01:03 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload test 00-04-96-4A-A7-08 upload-time 03/01/2014-12:30</td>
</tr>
<tr>
<td>Jan 31 00:59:57 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload cancel-upload all</td>
</tr>
<tr>
<td>Jan 31 00:59:23 2014</td>
<td>admin</td>
<td>192.168.100.225 46</td>
<td>captive-portal-page-upload test all exit</td>
</tr>
</tbody>
</table>
--More--
rfs7000-37FABE>service show diag stats on rfs7000-37FABE
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 on rfs7000-37FABE
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:
anald.log 1.3K Apr 4 10:48
```
Please export these files or delete them for more space.

rfs7000-37FABE>
rfs4000-229D58> 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>Sep 23 06:32:24 2014</td>
<td>5.7.0.0-028D</td>
<td>5.5.6.0-006D</td>
<td>Successful</td>
</tr>
<tr>
<td>Sep 17 05:34:30 2014</td>
<td>5.7.0.0-028D</td>
<td>5.5.6.0-005D</td>
<td>Successful</td>
</tr>
<tr>
<td>Sep 15 03:34:03 2014</td>
<td>5.7.0.0-026D</td>
<td>5.7.0.0-028D</td>
<td>Successful</td>
</tr>
<tr>
<td>Sep 08 03:37:44 2014</td>
<td>5.7.0.0-025D</td>
<td>5.7.0.0-026D</td>
<td>Successful</td>
</tr>
<tr>
<td>Sep 01 05:14:30 2014</td>
<td>5.7.0.0-024D</td>
<td>5.7.0.0-025D</td>
<td>Successful</td>
</tr>
<tr>
<td>Aug 25 04:49:25 2014</td>
<td>5.7.0.0-022D</td>
<td>5.7.0.0-024D</td>
<td>Successful</td>
</tr>
</tbody>
</table>
|--More--
rfs4000-229D58>
rfs4000-229D58> service show xpath-history

<table>
<thead>
<tr>
<th>DATE &amp; TIME</th>
<th>USER</th>
<th>XPATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Nov 11 14:11:00 2014</td>
<td>system</td>
<td>/wing-stats/device/00-23-68-22-9D-58/upgrade-history</td>
</tr>
<tr>
<td>Mon Nov 11 14:10:42 2014</td>
<td>system</td>
<td>/wing-stats/device/00-23-68-22-9D-58/system</td>
</tr>
<tr>
<td>Mon Nov 11 14:10:36 2014</td>
<td>system</td>
<td>/wing-stats/device/00-23-68-22-9D-58/system</td>
</tr>
</tbody>
</table>

rfs4000-229D58>
rfs7000-37FABE> service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
no country-code
!
wlan-qos-policy default
  no rate-limit wlan to-air
  no rate-limit wlan from-air
  no rate-limit client to-air
  no rate-limit client from-air
!
wlan wlan1
  ssid wlan1
  vlan 1
  qos-policy default
  encryption-type none
  authentication-type none
  no accounting radius
  no accounting syslog
rfs7000-37FABE>

System Information:

Free RAM: 68.0% (169 of 249) Min: 10.0%
File Descriptors: free: 24198 used: 960 max: 25500
CPU load averages: 1 min: 0.0% 5 min: 0.0% 15 min: 0.0%
Kernel Buffers:
Size:  32  64  128  256  512  1k  2k  4k  8k  16k  32k  64k  128k
Usage: 2761  2965  927  201  549  107  141  25  68  0  1  2  0
Limit: 32768  8192  4096  4096  8192  8192 16384 16384 1024  512  256  64  64

rfs4000-229D58#show adoption history on ap650-983278

<table>
<thead>
<tr>
<th>MAC</th>
<th>TYPE</th>
<th>EVENT</th>
<th>TIME_STAMP</th>
<th>REASON</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-23-68-22-9D-58</td>
<td>RFS4000</td>
<td>adopted</td>
<td>2014-02-21 11:37:37</td>
<td>N.A</td>
</tr>
</tbody>
</table>

rfs4000-229D58#

rfs4000-229D58#service clear adoption history on ap650-983278

rfs4000-229D58#show adoption history on ap650-983278

nx9500-6C8809#service analytics status

******************************************************************************
Analytics Service: Primary
******************************************************************************
WARNING: Please configure NFS. This is very important for data recovery and export!!
******************************************************************************
Analytics ip/dns configuration:
hdfs://127.0.0.1
127.0.0.1  127.0.0.1  localhost.localdomain   localhost nx9500-6C8809
******************************************************************************
Analytics last few commands history:
Sun Jul 21 23:18:40 UTC 2014 start
Thu Aug  1 23:39:43 UTC 2014 stop
Thu Aug  1 23:40:24 UTC 2014 stop
Thu Aug  1 23:43:19 UTC 2014 start
Fri Aug  2 00:49:47 UTC 2014 nfsserver
Fri Aug  2 00:50:06 UTC 2014 nfsserver
Fri Aug  2 00:53:04 UTC 2014 nfsserver
Fri Aug  2 00:53:25 UTC 2014 nfsserver
Fri Aug  2 01:05:21 UTC 2014 nfsserver
Fri Aug  2 03:58:39 UTC 2014 start
******************************************************************************
Process Name                   Status               PID
-------------------------------------------------------------------------------
hadoop-cli-datanode            running              3765
hadoop-cli-namenode            running              3899
hbase-cli-master               running              4061
hbase-cli-regionserver         running              3533
hbase-cli-zookeeper            running              3247
nx2manager                     running              14883
nxmonitor                      running              3098
remcp_name_daemon              running              25215
tomcat                         running              4296
******************************************************************************
nx9500-6C8809#

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>Aug 27 12:36:12 2014</td>
<td>team-urc</td>
<td>autostart</td>
</tr>
<tr>
<td>Aug 27 12:34:38 2014</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
<tr>
<td>Aug 19 18:51:01 2014</td>
<td>team-urc</td>
<td>autostart</td>
</tr>
<tr>
<td>Aug 19 18:49:27 2014</td>
<td>team-urc</td>
<td>stop (WiNG shutdown)</td>
</tr>
<tr>
<td>Aug 16 14:09:57 2014</td>
<td>team-vowlan</td>
<td>assign-usb-ports</td>
</tr>
<tr>
<td>Aug 06 12:46:50 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Aug 02 12:49:20 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Jul 22 12:24:09 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B>

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

nx4500-5CFA2B>

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>Aug 26 23:34:19 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Aug 16 00:25:33 2014</td>
<td>adsp</td>
<td>uninstall</td>
</tr>
<tr>
<td>Aug 14 01:46:16 2014</td>
<td>adsp</td>
<td>install</td>
</tr>
<tr>
<td>Aug 05 23:06:50 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Aug 01 23:43:19 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
<tr>
<td>Jul 21 23:18:39 2014</td>
<td>Domain-0</td>
<td>autostart</td>
</tr>
</tbody>
</table>

nx9500-6C874D>

The following examples show the service > analytics > wifi and service > analytics > status outputs on a NX9500 service platform:

nx9500-6C8809#service analytics wifi
Wifi data polling will be enabled. Please run status command to check Wifi data polling status.

nx9500-6C8809#

nx9500-6C8809#service show diag stats

fan 1 (System Fan 1) current speed: 2870 min_speed: 693 hysteresis: 250
fan 2 (System Fan 2) current speed: 3115 min_speed: 665 hysteresis: 250
fan 3 (System Fan 3) current speed: 2800 min_speed: 665 hysteresis: 250
fan 4 (System Fan 4) current speed: 3115 min_speed: 665 hysteresis: 250
fan 5 (System Fan 5) current speed: 6864 min_speed: 665 hysteresis: 250
fan 6 (System Fan 6) current speed: 6188 min_speed: 665 hysteresis: 250

Sensor 1 (Baseboard) Temperature 33.0 C
Sensor 2 (Front Panel) Temperature 24.0 C
Sensor 3 (PS1) Temperature 27.0 C
Sensor 4 (PS2) Temperature 30.0 C
Sensor 5 (HSBP) Temperature 25.0 C
nx9500-6C8809#service analytics status

*******************************************************************************
 Analytics Service: Primary
*******************************************************************************
WARNING: Please configure NFS. This is very important for data recovery and export!!
*******************************************************************************
Analytics ip/dns configuration:
hdfs://127.0.0.1
127.0.0.1  127.0.0.1  localhost.localdomain  localhost nx9500-6C8809
*******************************************************************************
Analytics last few commands history:
Thu Dec  5 04:12:08 UTC 2014 stop
Thu Dec  5 04:12:13 UTC 2014 stop
Thu Dec  5 04:12:19 UTC 2014 stop
Thu Dec  5 04:16:14 UTC 2014 start
Thu Dec  5 05:48:47 UTC 2014 stop
Thu Dec  5 05:50:34 UTC 2014 stop
Thu Dec  5 05:54:46 UTC 2014 start
Fri Dec  6 00:06:32 UTC 2014 stop
Fri Dec  6 00:08:16 UTC 2014 stop
Fri Dec  6 00:12:19 UTC 2014 start
*******************************************************************************
Process Name                   Status               PID
-------------------------------------------------------------------------------
hadoop-cli-datanode            running              4178
hadoop-cli-namenode            running              4306
hbase-cli-master               running              4466
hbase-cli-regionserver         running              3946
hbase-cli-zookeeper            running              3598
nx2manager                     running              4777
nxmonitor                      running              3455
remcp_name_daemon              running              5655
tomcat                         running              4701
*******************************************************************************
Analytics Polling : Enabled
*******************************************************************************
nx9500-6C8809#

nx4500-5CFA2B#service radio 1 adaptivity
nx4500-5CFA2B#

ap6522-C#service show wireless adaptivity-status

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>DETECTED</th>
<th>EXPIRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>0 days 01:36:59 ago</td>
<td>12181 secs</td>
</tr>
<tr>
<td>52</td>
<td>0 days 01:36:59 ago</td>
<td>12181 secs</td>
</tr>
<tr>
<td>60</td>
<td>0 days 02:13:38 ago</td>
<td>9982 secs</td>
</tr>
</tbody>
</table>

ap6522-C#
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show <PARAMETER>
```

**Parameters**

None

**Examples**

```
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
clock                       Display system clock
cluster                     Cluster Protocol
commands                    Show command lists
context                     Information about current context
critical-resources         Critical Resources
crypto                      Encryption related commands
debug                      Debugging functions
debugging                  Debugging functions
device-upgrade              Device Upgrade
dot1x                       802.1X
environmental-sensor       Display Environmental Sensor Module status
event-history               Display event history
event-system-policy        Display event system policy
file                        Display filesystem information
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
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
macauth                     MAC AUTH
mint                        MiNT protocol
ntp                         Network time protocol
password-encryption        Password encryption
power                       Show power over ethernet command
pppoe-client                PPP Over Ethernet client
privilege                   Show current privilege level
```
COMMON 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
terminal Display terminal configuration parameters
timezone The timezone
upgrade-status Display last image upgrade status
version Display software & hardware version
vrrp VRRP protocol
what Perform global search
wireless Wireless commands
wwan Display wireless WAN Status

rfs7000-37FABE#

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

write [memory|terminal]

Parameters

- write [memory|terminal]

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Writes to the non-volatile (NV) memory</td>
</tr>
<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.
### 6.1 show commands

Table 6.1 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 6-5</td>
</tr>
<tr>
<td>adoption</td>
<td>Displays information related to adoption</td>
<td>page 6-11</td>
</tr>
<tr>
<td>boot</td>
<td>Displays a device boot configuration</td>
<td>page 6-14</td>
</tr>
<tr>
<td>bonjour</td>
<td>Displays the configured Bonjour services available on local and remote sites</td>
<td>page 6-15</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Displays WLAN hotspot functions</td>
<td>page 6-16</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>clock</td>
<td>Displays the software system clock</td>
<td>page 6-23</td>
</tr>
<tr>
<td>cluster</td>
<td>Displays cluster commands</td>
<td>page 6-24</td>
</tr>
<tr>
<td>commands</td>
<td>Displays command list</td>
<td>page 6-25</td>
</tr>
<tr>
<td>context</td>
<td>Displays information about the current context</td>
<td>page 6-26</td>
</tr>
<tr>
<td>critical-resources</td>
<td>Displays critical resource information</td>
<td>page 6-27</td>
</tr>
<tr>
<td>crypto</td>
<td>Displays encryption mode information</td>
<td>page 6-28</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Displays device firmware upgradation information for devices adopted by a</td>
<td>page 6-31</td>
</tr>
<tr>
<td></td>
<td>wireless controller or access point</td>
<td></td>
</tr>
<tr>
<td>dot1x</td>
<td>Displays dot1x information on interfaces</td>
<td>page 6-34</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Displays environmental sensor's historical data (applicable only to AP8132)</td>
<td>page 6-36</td>
</tr>
<tr>
<td>event-history</td>
<td>Displays event history</td>
<td>page 6-40</td>
</tr>
<tr>
<td>event-system-policy</td>
<td>Displays event system policy configuration information</td>
<td>page 6-41</td>
</tr>
<tr>
<td>file</td>
<td>Displays file system information</td>
<td>page 6-42</td>
</tr>
<tr>
<td>firewall</td>
<td>Displays wireless firewall information</td>
<td>page 6-43</td>
</tr>
<tr>
<td>global</td>
<td>Displays global information for network devices based on the parameters</td>
<td>page 6-46</td>
</tr>
<tr>
<td>gre</td>
<td>Displays GRE tunnel related information</td>
<td>page 6-48</td>
</tr>
<tr>
<td>interface</td>
<td>Displays interface status</td>
<td>page 6-49</td>
</tr>
<tr>
<td>ip</td>
<td>Displays IP related information</td>
<td>page 6-53</td>
</tr>
<tr>
<td>ip-access-list</td>
<td>Displays IP access list statistics</td>
<td>page 6-59</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>l2tpv3</td>
<td>Displays Layer 2 Tunnel Protocol Version 3 (L2TPV3) information</td>
<td>page 6-61</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 6-64</td>
</tr>
<tr>
<td>licenses</td>
<td>Displays installed licenses and usage information</td>
<td>page 6-65</td>
</tr>
<tr>
<td>lldp</td>
<td>Displays Link Layer Discovery Protocol (LLDP) information</td>
<td>page 6-68</td>
</tr>
<tr>
<td>logging</td>
<td>Displays logging information</td>
<td>page 6-69</td>
</tr>
<tr>
<td>mac-access-list-stats</td>
<td>Displays MAC access list statistics</td>
<td>page 6-70</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Displays MAC address table entries</td>
<td>page 6-71</td>
</tr>
<tr>
<td>macauth</td>
<td>Displays details of wired ports that have MAC address-based authentication enabled</td>
<td>page 6-72</td>
</tr>
<tr>
<td>mint</td>
<td>Displays MiNT protocol configuration commands</td>
<td>page 6-74</td>
</tr>
<tr>
<td>ntp</td>
<td>Displays Network Time Protocol (NTP) information</td>
<td>page 6-77</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Displays password encryption status</td>
<td>page 6-78</td>
</tr>
<tr>
<td>power</td>
<td>Displays Power over Ethernet (PoE) information</td>
<td>page 6-79</td>
</tr>
<tr>
<td>pppoe-client</td>
<td>Displays Point to Point Protocol over Ethernet (PPPoE) client information</td>
<td>page 6-80</td>
</tr>
<tr>
<td>privilege</td>
<td>Displays current privilege level information</td>
<td>page 6-81</td>
</tr>
<tr>
<td>reload</td>
<td>Displays scheduled reload information</td>
<td>page 6-82</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Displays RF Domain manager selection details</td>
<td>page 6-83</td>
</tr>
<tr>
<td>role</td>
<td>Displays role-based firewall information</td>
<td>page 6-84</td>
</tr>
<tr>
<td>route-maps</td>
<td>Display route map statistics</td>
<td>page 6-85</td>
</tr>
<tr>
<td>rtls</td>
<td>Displays Real Time Location Service (RTLS) statistics of access points</td>
<td>page 6-86</td>
</tr>
<tr>
<td>running-config</td>
<td>Displays configuration file contents</td>
<td>page 6-87</td>
</tr>
<tr>
<td>session-changes</td>
<td>Displays configuration changes made in this session</td>
<td>page 6-93</td>
</tr>
<tr>
<td>session-config</td>
<td>Displays a list of currently active open sessions on the device</td>
<td>page 6-94</td>
</tr>
<tr>
<td>sessions</td>
<td>Displays CLI sessions</td>
<td>page 6-95</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 6-96</td>
</tr>
<tr>
<td>smart-rf</td>
<td>Displays Smart RF management commands</td>
<td>page 6-97</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Displays spanning tree information</td>
<td>page 6-100</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>startup-config</td>
<td>Displays complete startup configuration script on the console</td>
<td>page 6-103</td>
</tr>
<tr>
<td>terminal</td>
<td>Displays terminal configuration parameters</td>
<td>page 6-104</td>
</tr>
<tr>
<td>timezone</td>
<td>Displays timezone information for the system and managed devices</td>
<td>page 6-105</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Displays image upgrade status</td>
<td>page 6-106</td>
</tr>
<tr>
<td>version</td>
<td>Displays a device’s software and hardware version</td>
<td>page 6-107</td>
</tr>
<tr>
<td>vrrp</td>
<td>Displays Virtual Router Redundancy Protocol (VRRP) protocol details</td>
<td>page 6-108</td>
</tr>
<tr>
<td>what</td>
<td>Displays details of a specified search phrase</td>
<td>page 6-110</td>
</tr>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
<td>page 6-111</td>
</tr>
<tr>
<td>wwan</td>
<td>Displays the wireless WAN status</td>
<td>page 6-128</td>
</tr>
<tr>
<td>slot</td>
<td>Displays Peripheral Component Interconnect (PCI) express slot statistics</td>
<td>page 6-129</td>
</tr>
<tr>
<td>smart-cache</td>
<td>Displays details on the cached entry for a specific URL or all URLs</td>
<td>page 6-130</td>
</tr>
<tr>
<td>virtual-machine</td>
<td>Displays the virtual-machine (VM) configuration, logs, and statistics (applicable only to the NX45XX and NX65XX service platforms)</td>
<td>page 6-132</td>
</tr>
<tr>
<td>mirroring</td>
<td>Displays the port mirroring sessions (applicable only to the NX4524 and NX6524 service platforms)</td>
<td>page 6-135</td>
</tr>
<tr>
<td>raid</td>
<td>Displays Redundant Array of Independent Disks (RAID) related information, such as array status, consistency check status, and RAID log.</td>
<td>page 6-136</td>
</tr>
</tbody>
</table>
6.1.1 show

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show <PARAMETER>
```

Parameters

None

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 wireless controller
boot                        Display boot configuration.
bonjour                     Bonjour Gateway related commands
 captive-portal              Captive portal commands
 captive-portal-page-upload  Captive portal advanced page upload
 cdp                         Cisco Discovery Protocol
 clock                       Display system clock
 cluster                     Cluster Protocol
 commands                   Show command lists
 context                     Information about current context
 critical-resources          Critical Resources
 crypto                      Encryption related commands
 debug                       Debugging functions
 debugging                   Debugging functions
 device-upgrade              Device Upgrade
 dot1x                       802.1X
 environmental-sensor        Display Environmental Sensor Module status
 event-history               Display event history
 event-system-policy         Display event system policy
 file                        Display filesystem information
 firewall                    Wireless Firewall
 global                      Global-level information
 gre                         Displays gre related information
 interface                   Interface Configuration/Statistics commands
 ip                          Internet Protocol (IP)
 ip-access-list              IP 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
 macauth                     MAC AUTH
 mint                        MiNT protocol
 mirroring                   Show mirroring sessions
```
ntp                         Network time protocol
password-encryption        Password encryption
power                      Show power over ethernet command
pppoe-client               PPP Over Ethernet client
privilege                   Show current privilege level
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
rtl                        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
terminal                   Display terminal configuration parameters
timezone                   The timezone
upgrade-status             Display last image upgrade status
version                    Display software & hardware version
virtual-machine            Virtual Machine
vrrp                       VRRP protocol
what                       Perform global search
wireless                   Wireless commands
wwan                       Display wireless WAN Status
                           
<DEVICE>(config)#
                           
rfs7000-37FABE(config)#show clock
2014-02-15 15:28:26 UTC
rfs7000-37FABE(config)#

PRIVILEGE EXEC Mode
<DEVICE>#show ?
                           adoption                      Display information related to adoption to
                           boot                         Display boot configuration.
                           bonjour                      Bonjour Gateway related commands
                           captive-portal              Captive portal commands
                           captive-portal-page-upload  Captive portal advanced page upload
                           cdp                          Cisco Discovery Protocol
clock                      Display system clock
cluster                    Cluster Protocol
commands                   Show command lists
context                    Information about current context
critical-resources        Critical Resources
crypto                     Encryption related commands
debug                      Debugging functions
debugging                  Debugging functions
device-upgrade             Device Upgrade
dot1x                       802.1X
environmental-sensor       Display Environmental Sensor Module status
event-history              Display event history
event-system-policy       Display event system policy
file                       Display filesystem information
firewall                   Wireless Firewall
global                     Global-level information
gre                        Negate a command or set its defaults
interface                  Interface Configuration/Statistics commands
ip                         Internet Protocol (IP)
ip-access-list            IP ACL
l2tpv3                     L2TPv3 information
ldap-agent                 LDAP Agent Configuration
licenses
lldp
logging
mac-access-list
mac-address-table
macauth
mint
mirroring
ntp
password-encryption
power
pppoe-client
privilege
raid
reload
remote-debug
rf-domain-manager
role
route-maps
rtls
running-config
session-changes
session-config
sessions
site-config-diff
slot
smart-cache
smart-rf
spanning-tree
startup-config
terminal
timezone
upgrade-status
version
virtual-machine
vrrp
what
wireless
wwan

<DEVICE>#
rfs7000-37FABE# show terminal
Terminal Type: xterm
Length: 24     Width: 80
rfs7000-37FABE#

USER EXEC Mode
<DEVICE>>show ?
adoption
boot
bonjour
captive-portal
captive-portal-page-upload
cdp
clock
cluster
commands
context
critical-resources
crypto
debbug
debbuging
device-upgrade
dotix
environmental-sensor
event-history
event-system-policy

Display information related to adoption to wireless controller
Display boot configuration.
Bonjour Gateway related commands
Captive portal commands
Captive portal advanced page upload
Cisco Discovery Protocol
Display system clock
Cluster Protocol
Show command lists
Information about current context
Critical Resources
Encryption related commands
Debugging functions
Debugging functions
Device Upgrade
802.1X
Display Environmental Sensor Module status
Display event history
Display event system policy
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>ap7131-889EC4</td>
<td>00-15-70-88-9E-C4</td>
<td>default-ap7131</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>2</td>
<td>ap300-CF1EDA</td>
<td>00-A0-F8-CF-1E-DA</td>
<td>default-ap300</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>3</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>4</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>5</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>6</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>7</td>
<td>ap6521-08736B</td>
<td>5C-0E-8B-08-73-6B</td>
<td>default-ap6521</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>8</td>
<td>ap6522-7BF224</td>
<td>5C-0E-8B-7B-F2-24</td>
<td>default-ap6522</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>9</td>
<td>ap6532-31659</td>
<td>00-23-68-31-16-59</td>
<td>default-ap6532</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>10</td>
<td>ap6562-0E1260</td>
<td>00-23-09-0E-12-60</td>
<td>default-ap6562</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>11</td>
<td>ap7131-99BFA8</td>
<td>00-23-68-99-BF-A8</td>
<td>default-ap71xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>12</td>
<td>ap8132-BEF116</td>
<td>C4-01-FA-BE-F1-16</td>
<td>default-ap81xx</td>
<td>default</td>
<td>un-adopted</td>
</tr>
<tr>
<td>13</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)#
The following Show commands are specific to the NX45XX and NX65XX series service platforms:

nx4500-5CFA2B>show slot
----------------------------
SLOT TYPE MODULE   STATUS
----------------------------
 1    []   wing   Enabled
 2    []   wing   Enabled
 3    []   wing   Enabled
 4    []   wing   Enabled
----------------------------
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
-------------------------
USED    TOTAL    USAGE
-------------------------
 1592   33554432   0%
-------------------------
nx4500-5CFA2B#

nx4500-5CFA2B(config)#show smart-cache statistics
------------------------------
DURATION | DATA (KB) | BANDWIDTH (Kbps) | REQUESTS
---|---|---|---
Since boot | 0 | 0 | 0 | 0
------------------------------
nx4500-5CFA2B(config)#

nx4500-5CFA2B(config)#show virtual-machine statistics
-----------------------------------------------
NAME           STATE       VCPUS MEM (MB)   BRIDGE-IF           IP
-----------------------------------------------
team-rls      (not_installed)   -     -        -              -
team-urc      Running           1     1200     eth0 (vmif2)   192.168.13.103
team-vowlan   (not_installed)   -     -        -              -
-----------------------------------------------
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: Sat Sep 14 06:00:03 2014
  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:

```bash
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>

```
x9500-6C874D(config)#
```
6.1.2 adoption

Displays adoption related information, and is common to the User Exec, Priv Exec, and Global Config modes.

In a 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, or NX9510.
- Site controller – NX45XX, NX65XX, RFS7000, RFS6000, or RFS4000.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show adoption offline
show adoption config-errors <DEVICE-NAME>
show adoption log [adoptee|adopter] {on <DEVICE-NAME>}
show adoption [controllers|history|info|pending|status|timeline] {on <DEVICE-NAME>}
```

Parameters

- `show adoption offline` Displays non-adopted status of the logged device and its adopted access points
- `show adoption config-errors <DEVICE-NAME>` Displays configuration errors for a specified adopted device
- `show adoption log [adoptee|adopter] {on <DEVICE-NAME>}` Displays adoption related information. It also displays configuration errors.
log [adoptee|adopter] {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, 2014-01-19 22:00:13:MLCP_TAG_CLUSTER_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

- **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 adoptee device’s MAC address.

    Specify the adoptee 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. 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.

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show adoption [history</td>
<td>controllers</td>
</tr>
<tr>
<td>adoption</td>
<td>Displays information about adopted controllers. This is applicable in a Hierarchically managed network, where site controllers are adopted by the NOC controllers.</td>
</tr>
<tr>
<td>controllers</td>
<td>Displays adoption history of the logged device and its adopted access points</td>
</tr>
<tr>
<td>history</td>
<td>Displays adoption status for logged devices</td>
</tr>
<tr>
<td>info</td>
<td>Displays adopted device information</td>
</tr>
<tr>
<td>pending</td>
<td>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 &lt;device-name&gt; option to specify the device.</td>
</tr>
<tr>
<td>timeline</td>
<td>The following keywords are common to all of the above parameters:</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>on &lt;DEVICE-NAME&gt; – Optional. Displays a device’s adoption information, based on the parameter passed.</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(config)#show adoption offline
---

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOST-NAME</th>
<th>TYPE</th>
<th>RF-DOMAIN</th>
<th>TIME OFFLINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>5C-0E-8B-E3-C3-56</td>
<td>ap621-E3C356</td>
<td>ap621</td>
<td>default</td>
<td>unknown</td>
</tr>
<tr>
<td>00-A0-F8-CF-1E-DA</td>
<td>ap300-CF1EDA</td>
<td>ap300</td>
<td>(un-mapped)</td>
<td>unknown</td>
</tr>
</tbody>
</table>
---

Total number of devices displayed: 2
```

```
rfs4000-229D58(config)#show adoption log adoptee
---
2014-03-15 12:47:07:DNS resolution completed, starting MLCP
2014-03-15 12:47:07:Received 0 hostnames through option 192
2014-03-15 12:47:07:Changing adoption state from Disabled to No adopters found
2014-03-15 12:47:07:DNS resolution completed, starting MLCP
2014-03-15 12:47:07:Adoption enabled due to configuration
```

```
rfs4000-229D58(config)#show adoption controllers
---

<table>
<thead>
<tr>
<th>ADOPTED-BY</th>
<th>NAME</th>
<th>RF-DOMAIN</th>
<th>MAC</th>
<th>MINT-ID</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rfs4000-229BA0</td>
<td>rfs4k</td>
<td>00-23-68-22-9B-A0</td>
<td>68.22.9B.A0</td>
<td>192.168.200.70</td>
</tr>
<tr>
<td></td>
<td>rfs7000-37FA7D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx6524-4A8814</td>
<td>bob</td>
<td>B4-C7-99-4A-88-14</td>
<td>19.4A.88.14</td>
<td>192.168.200.72</td>
</tr>
<tr>
<td></td>
<td>rfs7000-19C875</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>rfs4000-6FA2D4</td>
<td>rfs4k</td>
<td>B4-C7-99-6F-A2-D4</td>
<td>19.6F.A2.D4</td>
<td>192.168.200.71</td>
</tr>
<tr>
<td></td>
<td>rfs7000-19C875</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
---

Total number of devices displayed: 3
```

```
rfs7000-19C875>
```
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show boot {on <DEVICE-NAME>}
```

**Parameters**

- `show boot {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Parameter</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 &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays a specified device's boot configuration</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**

```
rfs4000-229D58(config)#show boot

+---------------+---------------+---------------+-------------+
| IMAGE         | BUILD DATE    | INSTALL DATE  | VERSION     |
|---------------+---------------+---------------+-------------+
| Secondary     | 06:29:2014  00:36:59 | 06:30:2014 08:56:11 | 5.5.6.0-005D |
+---------------+---------------+---------------+-------------+

Current Boot : Primary
Next Boot     : Primary
Software Fallback : Enabled
rfs4000-229D58(config)#
```
### 6.1.4 bonjour

Displays the configured Bonjour services available on local and remote sites.

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS7000

**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>
</tbody>
</table>

- `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

**Examples**

```
rfs7000-37FAEBE#show bonjour services on ap7131-11E6C4
```

<table>
<thead>
<tr>
<th>SERVICE_NAME</th>
<th>INSTANCE_NAME</th>
<th>IP:PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>_universal._sub._ipp._tcp.local</td>
<td>Brother MFC-8510DN._ipp._tcp.local</td>
<td>32.32.32.103:631 32 Local</td>
</tr>
<tr>
<td>32.32.32.103:631 32 Local</td>
<td>HP MFP M425dn Service :)._ipp._tcp.local</td>
<td>32.32.32.104:631 32 Local</td>
</tr>
<tr>
<td>32.32.32.103:631 32 Local</td>
<td>Officejet Pro 8100 [08159B]._ipp._tcp.local</td>
<td>32.32.32.105:631 32 Local</td>
</tr>
<tr>
<td>_universal._sub._ipp._tcp.local</td>
<td>Apple TV._airplay._tcp.local</td>
<td>32.32.32.101:7000 32 Local</td>
</tr>
<tr>
<td>32.32.32.103:631 32 Local</td>
<td>B8782E2D922E@Apple TV._raop._tcp.local</td>
<td>32.32.32.101:5000 32 Local</td>
</tr>
<tr>
<td>_ipp._tcp.local</td>
<td>HP MFP M425dn Service :)._ipp._tcp.local</td>
<td>32.32.32.104:631 32 Local</td>
</tr>
<tr>
<td>32.32.32.105:631 32 Local</td>
<td>Officejet Pro 8100 [08159B]._ipp._tcp.local</td>
<td>32.32.32.105:631 32 Local</td>
</tr>
</tbody>
</table>

```
rfs7000-37FAEBE#```
6.1.5 captive-portal

show commands

Displays WLAN captive portal information. Use this command to view a configured captive portal's client information.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

show captive-portal client {filter|on|statistics}
show captive-portal client {filter} {captive-portal|ip|state|vlan|wlan}
show captive-portal client {filter} {captive-portal <CAPTIVE-PORTAL>|
not <CAPTIVE-PORTAL>}
show captive-portal client {filter} {ip <IP>|not <IP>}
show captive-portal client {filter} {state pending|success|not pending|success}
show captive-portal client {filter} {vlan <VLAN-ID>|not <VLAN-ID>}
show captive-portal client {filter} {wlan <WLAN-NAME>|not <WLAN-NAME>}
show captive-portal client {on <DEVICE-OR-DOMAIN-NAME>|statistics} {filter}
captive-portal|ip|state|vlan|wlan

Parameters

- show captive-portal client {filter} {captive-portal <CAPTIVE-PORTAL>|
not <CAPTIVE-PORTAL>}

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Optional. Defines additional filters</td>
</tr>
</tbody>
</table>

- show captive-portal client {filter} {ip <IP>|not <IP>}

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Optional. Defines additional filters</td>
</tr>
<tr>
<td>ip &lt;IP&gt;</td>
<td>not &lt;IP&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- show captive-portal client {filter} {state pending|success|not pending|success}|

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Optional. Defines additional filters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Optional. Defines additional filters</td>
</tr>
<tr>
<td>state</td>
<td>Optional. Filters clients based on their state of authentication</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>pending</td>
<td>Displays clients redirected for authentication</td>
</tr>
<tr>
<td>success</td>
<td>Displays successfully authenticated clients</td>
</tr>
<tr>
<td>not [pending</td>
<td>success]]</td>
</tr>
<tr>
<td>• pending</td>
<td>Displays successfully authenticated clients (opposite of pending authentication)</td>
</tr>
<tr>
<td>• success</td>
<td>Displays clients redirected for authentication (opposite of successful authentication)</td>
</tr>
</tbody>
</table>

- **show captive-portal client {filter} {vlan [<VLAN-ID>|not <VLAN-ID>]}

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Optional. Defines additional filters</td>
</tr>
<tr>
<td>vlan [&lt;VLAN-ID&gt;]</td>
<td>Optional. Displays captive portal clients based on the VLAN ID passed</td>
</tr>
<tr>
<td>not &lt;VLAN-ID&gt;]</td>
<td>• &lt;VLAN-ID&gt; – Specify the VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>• not &lt;VLAN-ID&gt; – Inverts match selection</td>
</tr>
</tbody>
</table>

- **show captive-portal client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]}

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Optional. Defines additional filters</td>
</tr>
<tr>
<td>wlan [&lt;WLAN-NAME&gt;]</td>
<td>Optional. Displays captive portal clients based on the WLAN name passed</td>
</tr>
<tr>
<td>not &lt;WLAN-NAME&gt;]</td>
<td>• &lt;WLAN-NAME&gt; – Specify the WLAN name.</td>
</tr>
<tr>
<td></td>
<td>• not &lt;WLAN-NAME&gt; – Inverts match selection</td>
</tr>
</tbody>
</table>

- **show captive-portal client {on <DEVICE-OR-DOMAIN-NAME>|statistics} {filter} {captive-portal/ip/state|vlan|wlan}

<table>
<thead>
<tr>
<th>captive-portal client</th>
<th>Displays captive portal client information</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>Optional. Displays captive portal clients 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>statistics</td>
<td>Optional. Displays captive portal client statistics. This feature enables monitoring of a captive portal client’s data usage. When enabled, it provides a client’s data transmission (both upstream and downstream) details, without considering the dot11 overhead for each packet.</td>
</tr>
<tr>
<td>filter</td>
<td>The following keywords are common to the ‘on’ and ‘statistics’ parameters:</td>
</tr>
<tr>
<td>• filter – Optional. Defines additional filters</td>
<td></td>
</tr>
<tr>
<td>• captive-portal – Optional. Displays captive portal client information for a specified captive portal</td>
<td></td>
</tr>
<tr>
<td>• ip – Optional. Displays captive portal client information based on IP address passed</td>
<td></td>
</tr>
<tr>
<td>• state – Optional. Displays captive portal client information based on the their authentication state</td>
<td></td>
</tr>
<tr>
<td>• vlan – Displays captive portal clients on a specified VLAN</td>
<td></td>
</tr>
<tr>
<td>• wlan – Optional. Displays captive portal clients on a specified WLAN</td>
<td></td>
</tr>
</tbody>
</table>
Examples

rfs4000-229D58#show captive-portal client
===========================================================================
RF-Domain: test
CLIENT                     IP     CAPTIVE-PORTAL     WLAN               VLAN         STATE
SESSION TIME
---------------------------------------------------------------------------------------
44-6D-57-08-25-4A    10.10.10.183 test               wlan-ap7131-cp     1          Pending 0:00:00
---------------------------------------------------------------------------------------
RF-Domain: test, sub-total of captive portal clients displayed = 1
===========================================================================
===========================================================================
RF-Domain: default
CLIENT                     IP     CAPTIVE-PORTAL     WLAN               VLAN         STATE
SESSION TIME
---------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------
RF-Domain: default, sub-total of captive portal clients displayed = 0
===========================================================================
===========================================================================
RF-Domain: new-l3-rf-dmn
CLIENT                     IP     CAPTIVE-PORTAL     WLAN               VLAN         STATE
SESSION TIME
---------------------------------------------------------------------------------------
00-24-D7-EC-CF-78    10.10.10.175 CP1                rfs-with-radio     1          Success 22:50:38
---------------------------------------------------------------------------------------
RF-Domain: new-l3-rf-dmn, sub-total of captive portal clients displayed = 1
===========================================================================
Total number of captive portal clients displayed: 2
rfs4000-229D58#

rfs4000-229D58#show captive-portal client statistics
===========================================================================
RF-Domain: test
CLIENT                     IP     CAPTIVE-PORTAL          TX-PKTS     TX-BYTES      RX-PKTS     RX-BYTES
---------------------------------------------------------------------------------------
44-6D-57-08-25-4A    10.10.10.183 test                          0            0            0
---------------------------------------------------------------------------------------
RF-Domain: test, sub-total of captive portal clients displayed = 1
===========================================================================
===========================================================================
RF-Domain: default
CLIENT                     IP     CAPTIVE-PORTAL          TX-PKTS     TX-BYTES      RX-PKTS     RX-BYTES
---------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------
RF-Domain: default, sub-total of captive portal clients displayed = 0
===========================================================================
===========================================================================
<table>
<thead>
<tr>
<th>CLIENT</th>
<th>IP</th>
<th>CAPTIVE-PORTAL</th>
<th>TX-PKTS</th>
<th>TX-BYTES</th>
<th>RX-PKTS</th>
<th>RX-BYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-24-D7-EC-CF-78</td>
<td>10.10.10.175</td>
<td>CP1</td>
<td>119</td>
<td>11419</td>
<td>26554</td>
<td>1396167</td>
</tr>
</tbody>
</table>

RF-Domain: new-l3-rf-dmn, sub-total of captive portal clients displayed = 1

Total number of captive portal clients displayed: 2
6.1.6 captive-portal-page-upload

Display commands
Displays captive portal page information, such as upload history, upload status, and page file download status

Supported in the following platforms:
- Access Points — AP300, 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, 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

<table>
<thead>
<tr>
<th>load-image-status</th>
<th>Displays captive portal advanced page file download status on the logged device</th>
</tr>
</thead>
</table>
- show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}

<table>
<thead>
<tr>
<th>history {on &lt;RF-DOMAIN-NAME&gt;}</th>
<th>Displays captive portal page upload history</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;RF-DOMAIN-NAME&gt; — Optional. Displays captive portal page upload history within a specified RF Domain. Specify the RF Domain name.</td>
<td></td>
</tr>
</tbody>
</table>

- show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>|<RF-DOMAIN-MANAGER>]}

<table>
<thead>
<tr>
<th>status {on &lt;RF-DOMAIN-NAME&gt;</th>
<th>Displays captive portal page upload status</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;RF-DOMAIN-NAME&gt; — Optional. Displays captive portal page upload status within a specified RF Domain. Specify the RF Domain name.</td>
<td></td>
</tr>
<tr>
<td>on &lt;RF-DOMAIN-MANAGER&gt; — Optional. Displays captive portal page upload status for a specified RF Domain Manager. Specify the RF Domain Manager name.</td>
<td></td>
</tr>
</tbody>
</table>

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

Displays the Cisco Discovery Protocol (CDP) neighbor table

Supported in the following platforms:
- Access Points — AP300, 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, 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.
  - 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:

```
 rfs7000-37FABE(config)#show cdp neighbors detail
 -------------------------
 Device ID: ap7131-11E6C4
 Entry address(es):
   IP Address: 172.16.10.23
   IP Address: 172.16.20.1
   IP Address: 169.254.230.196
 Platform: AP7131, Capabilities: Router Switch
 Interface: ge1, Port ID (outgoing port): ge1
 Hold Time: 131 sec
 advertisement version: 2
 Native VLAN: 1
 Duplex: full
 Version: 5.4.1.0-018R
 -------------------------
 Device ID: ap7131-139B34
 Entry address(es):
   IP Address: 172.16.10.22
 Platform: AP7131N, Capabilities: Router Switch
 Interface: ge1, Port ID (outgoing port): ge1
 Hold Time: 129 sec

--More--
```

rfs7000-37FABE(config)#
The following example shows a non-detailed CDP neighbors table:

rfs7000-37FABE(config)#show cdp neighbors

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Neighbor IP</th>
<th>Platform</th>
<th>Local Interface</th>
<th>Port ID</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap7131-11E6C4</td>
<td>172.16.10.23</td>
<td>AP7131</td>
<td>ge1</td>
<td>ge1</td>
<td>full</td>
</tr>
<tr>
<td>ap7131-139B34</td>
<td>172.16.10.22</td>
<td>AP7131N</td>
<td>ge1</td>
<td>ge1</td>
<td>full</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#
### 6.1.8 clock

- **show commands**

Displays a selected system’s clock

Supported in the following platforms:

- Access Points — AP300, 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, 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</td>
</tr>
<tr>
<td></td>
<td>platform, or RF Domain.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#show clock
2014-02-15 15:38:47 UTC
rfs7000-37FABE(config)#
```

```
6.1.9 cluster

show commands

Displays cluster information (cluster configuration parameters, members, status etc.)

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Displays cluster information</td>
</tr>
<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

Cluster Configuration Information
Name : Cluster1
Configured Mode : Active
Master Priority : 128
Force configured state : Disabled
Force configured state delay : 5 minutes
Handle STP : Disabled

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>70.37.FA.BE</td>
<td>00-15-70-37-FA-BE</td>
<td>Active</td>
<td>0</td>
<td>0</td>
<td>50</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>5.4.2.0-006D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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)#
6.1.10 commands

Displays commands available for the current mode

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```show commands```

Parameters

None

Examples

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 cfgd
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)#

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 cfgd
show debugging fib (|(on DEVICE-NAME))
show debugging adoption (|(on DEVICE-OR-DOMAIN-NAME))
show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
--More--
nx4500-5CFA2B(config)#
6.1.11 context

Displays the current context details.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show context {include-factory|session-config {include-factory}}
```

Parameters

- `include-factory` Optional. Includes factory defaults
- `session-config include-factory` Optional. Displays running system information in the current context

Examples

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.5.6.0-006D
!
! 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)#
```
### 6.1.12 critical-resources

- **show commands**

Displays critical resource information. Critical resources are resources vital to the network.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show critical-resources {on <DEVICE-NAME>}
```

**Parameters**

- `critical-resources` Displays critical resources information
- `on <DEVICE-NAME>` Optional. Displays critical resource information on a specified device
  - `<DEVICE-NAME>` — Specify the name of the AP, wireless controller, or service platform.

**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)#
```
6.1.13 crypto

show commands

Displays encryption mode information

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

show crypto [ike|ipsec|key|pki]
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} {on <DEVICE-NAME>}
show crypto ipsec sa {peer <IP>} {detail} {on <DEVICE-NAME>}
show crypto key rsa {on|public-key-detail} {on <DEVICE-NAME>}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all|on} {on <DEVICE-NAME>}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}

Parameters
- show crypto ike sa {detail|peer <IP>} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>crypto ike sa</th>
<th>Displays Internet Key Exchange (IKE) security association (SA) statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays detailed IKE SA statistics</td>
</tr>
<tr>
<td>peer &lt;IP&gt;</td>
<td>Optional. Displays IKE SA statistics for a specified peer</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays IKE SA statistics on a specified device</td>
</tr>
<tr>
<td>version [1</td>
<td>2]</td>
</tr>
<tr>
<td>peer &lt;IP&gt;</td>
<td>Optional. Displays IKE SA version statistics for a specified peer</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keyword is recursive and common to the 'peer ip' parameter:</td>
</tr>
</tbody>
</table>

| The following keyword is recursive and common to the 'peer ip' parameter: |
| 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 ipsec sa** {detail} {on <DEVICE-NAME>}

  **crypto ipsec sa** Displays Internet Protocol Security (IPSec) SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session.

  **detail** Optional. Displays detailed IPSec SA statistics.

  **on <DEVICE-NAME>** Optional. Displays IPSec SAs on a specified device.

    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

- **show crypto sa** {peer <IP>} {detail} {on <DEVICE-NAME>}

  **crypto ipsec sa** Displays IPSec SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session.

  **peer <IP>** detail Optional. Displays IPSec SA statistics for a specified peer.

    - **<IP>** – Specify the peer’s IP address in the A.B.C.D format.
    - **detail** – Displays detailed IPSec SA statistics for the specified peer.

  **on <DEVICE-NAME>** The following keyword is recursive:

    - **on <DEVICE-NAME>** – Optional. Displays IPSec SAs on a specified device.

    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

- **show crypto key rsa** {public-key-detail} {on <DEVICE-NAME>}

  **crypto key rsa** Displays RSA public keys.

  **public-key-detail** Optional. Displays public key in the Privacy-Enhanced Mail (PEM) format.

  **on <DEVICE-NAME>** The following keyword is recursive:

    - **on <DEVICE-NAME>** – Optional. Displays public key on a specified device.

    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.

- **show crypto pki trustpoints** {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}

  **crypto pki** Displays PKI related information.

  **trustpoints** Displays WLAN trustpoints.

  **<TRUSTPOINT-NAME>** Optional. Displays a specified trustpoint details. Specify the trustpoint name.

  **all** Optional. Displays details of all trustpoints.

  **on <DEVICE-NAME>** The following keyword is recursive and common to the ‘trustpoint-name’ and ‘all’ parameters:

    - **on <DEVICE-NAME>** – Optional. Displays trustpoints configured on a specified device.

    - **<DEVICE-NAME>** – Specify the name of the AP, wireless controller, or service platform.
Examples

rfs7000-37FABE(config)#show crypto key rsa public-key-detail

RSA key name: test1        Key-length: 1032
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQL+qxgk4HLK7XRKokIinDCiRiAz
rE1aUGMi19iQJGSQakhV3WxP1V8NsRn1uhojPMoBYTddAgOTgNnQxvrMond7y+3
1XQomy3Xb0wLj0KSp6CPOZgXHbWrUSNP3K7fNAKSYjQ0LlAJTcvtIKRe0yfLCSsJd
9HZF4HxumlkOfy93wIDAQAB
-----END PUBLIC KEY-----

RSA key name: mint_security_trustpoint-srvr-priv-key        Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/zlGeiIM0YagLvkvIEFQnd/lf
6aw1S+xQN1DugLJQgA27ylNCtM5YeUKQD+lmljCvX9Ku+bAxLnVWF3PvttZgsH
J3d0ytzded/JuRJYCO2ChWYo0dTsufuyK/srzkJU2akiOyp9jCXUeLA8w1RRUBE
cNeRYDqQEoCHImmhwIDAQAB
-----END PUBLIC KEY-----

RSA key name: default-trustpoint-srvr-priv-key        Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGHBR2bxLeRZ4G6hm7jHJRsaAY
A216r4s4gptk2+ld+KemhPTFBVylk1dITkzF1EU70v0vKzant0pyAmdJ8ci/
--More--
rfs7000-37FABE(config)#show crypto key rsa
<table>
<thead>
<tr>
<th>#</th>
<th>KEY NAME</th>
<th>KEY LENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default-trustpoint-srvr-priv-key</td>
<td>1024</td>
</tr>
<tr>
<td>2</td>
<td>default_rsa_key</td>
<td>1024</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show crypto pki trustpoints all

Trustpoint Name: mint_security_trustpoint        (on-board CA)

-----------------------------------------------
CRL present: no
Server Certificate details:
  Key used: mint_security_trustpoint-srvr-priv-key
  Serial Number: 7037fabe03
  Subject Name:
    CN=70.37.fa.be, C=US, O=Company
  Issuer Name:
    CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Company
  Valid From : Mon Apr 26 15:00:41 2010 UTC
  Valid Until: Tue Apr 26 15:00:41 2011 UTC
CA Certificate details:
  Serial Number: 01
  Subject Name:
    CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Company
  Issuer Name:
    CN=70.37.fa.be:2010-04-26-15-00-39, C=US, O=Company
  Valid From : Mon Apr 26 15:00:39 2010 UTC
  Valid Until: Tue Apr 26 15:00:39 2011 UTC
--More--
rfs7000-37FABE(config)#
6.1.14 device-upgrade

Displays device firmware upgradation information for devices adopted by a wireless controller or access point.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```bash
show device-upgrade [history|load-image-status|status|versions]
```

Parameters

- show device-upgrade [history|load-image-status|status|versions]

<table>
<thead>
<tr>
<th>device-upgrade</th>
<th>Displays device upgrade information based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>Displays device upgrade history</td>
</tr>
</tbody>
</table>
| load-image-status | Displays firmware image loading status. The output displays the <DEVICE> image loading status in percentage.  
For example: #show device-upgrade load-image-status  
Download of ap81xx firmware file is 47 percent complete |
| status         | Displays device firmware upgrade status                      |
| versions       | Displays firmware image versions                              |

Examples

```bash
rfs4000-229D58#show device-upgrade versions
```

```text
-----------------------------------------------
CONTROLLER DEVICE-TYPE VERSION
-----------------------------------------------
  rfs4000-229D58 ap621 5.5.6.0-006D
  rfs4000-229D58 ap622 5.5.6.0-006D
  rfs4000-229D58 ap650 5.5.6.0-006D
  rfs4000-229D58 ap6511 none
  rfs4000-229D58 ap6521 5.5.6.0-006D
  rfs4000-229D58 ap6522 5.5.6.0-006D
  rfs4000-229D58 ap6532 5.5.6.0-006D
  rfs4000-229D58 ap6562 5.5.6.0-006D
  rfs4000-229D58 ap71xx none
  rfs4000-229D58 ap81xx none
  rfs4000-229D58 ap82xx none
  rfs4000-229D58 rfs4000 none
```

```bash
rfs4000-229D58#
```

```bash
rfs4000-6F8D1C#show device-upgrade summary
```

Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 2
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 1

-----------------------------------------------

rfs4000-6F8D1C#show device-upgrade status
DEVICE      STATE   UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR
UPGRADED BY
-----------------------------------------------------------------------------------------------
ap71xx-0B8638 rebooting immediate immediate 0 0  -   rfs4000-6F8D1C
ap650-311445 rebooting immediate immediate 0 0  -   rfs4000-6F8D1C
-----------------------------------------------------------------------------------------------
rfs4000-6F8D1C#show device-upgrade status
DEVICE      STATE   UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR
UPGRADED BY
-----------------------------------------------------------------------------------------------
ap71xx-0B863C failed  immediate  immediate 0 3  Start Upgrade failed
rfs4000-6F8D1C
-----------------------------------------------------------------------------------------------
rfs4000-6F8D1C#
rfs4000-229D58#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>ap6532-986C50</td>
<td>failed</td>
<td>2012-01-05 00:26:31</td>
<td>3</td>
<td>rfs4000-229D58</td>
<td>Update error: Bad file, failure in tar. tar: invalid tar magic</td>
</tr>
<tr>
<td>ap71xx-0F43D8</td>
<td>failed</td>
<td>2012-01-05 00:21:08</td>
<td>3</td>
<td>rfs4000-229D58</td>
<td>Update error: Unable to get update file, failure in ftp/openssl/tar</td>
</tr>
</tbody>
</table>

Total number of entries displayed: 2

rfs4000-229D58#

rfs4000-229D58#show device-upgrade status

'Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 0

rfs4000-229D58#

nx4500-5CFA2B(config)#show device-upgrade versions

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>DEVICE-TYPE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap621</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap622</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap650</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap6511</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap6521</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap6522</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap6532</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap6562</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap71xx</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap81xx</td>
<td>5.5.6.0-006D</td>
</tr>
<tr>
<td>nx4500-5CFA2B</td>
<td>ap92xx</td>
<td>5.5.6.0-006D</td>
</tr>
</tbody>
</table>

nx4500-5CFA2B(config)#
6.1.15 **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** — AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, 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, AP7502, AP7522, 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, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, 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 {on <DEVICE-NAME>}|on <DEVICE-NAME>}**

<table>
<thead>
<tr>
<th><strong>dot1x all</strong> {on &lt;DEVICE-NAME&gt;}</th>
<th>Optional. Displays dot1x information for all interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Displays dot1x information for all interfaces 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>

- **show dot1x {interface [<INTERFACE-NAME>|ge 1-4|port-channel 1-2]} {on <DEVICE-NAME>**

<table>
<thead>
<tr>
<th><strong>dot1x</strong> {on &lt;DEVICE-NAME&gt;}</th>
<th>Optional. Displays dot1x information for interfaces on a specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td>- &lt;DEVICE-NAME&gt; – Specify the name of AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

- **show dot1x {interface [<INTERFACE-NAME>|ge 1-4|port-channel 1-2]} {on <DEVICE-NAME>**

<table>
<thead>
<tr>
<th><strong>dot1x interface</strong></th>
<th>Optional. Displays dot1x information for a specified interface or interface type</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;INTERFACE-NAME&gt;</td>
<td>Displays dot1x information for the layer 2 (Ethernet port) interface specified by the &lt;INTERFACE-NAME&gt; parameter</td>
</tr>
</tbody>
</table>
**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

--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
```

*ge <1-4>*
Displays dot1x for a specified GigabitEthernet interface

*port-channel <1-2>*
Displays dot1x for a specified port channel interface

*on <DEVICE-NAME>*
The following keywords are common to all of the above parameters:

*<DEVICE-NAME>* – Specify the name of AP, wireless controller, or service platform.
### 6.1.16 environmental-sensor

#### show commands

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**
```
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>}`
- `show environmental-sensor [humidity|light|motion|summary|temperature|version]`

---

**environmental-sensor history**

Displays environmental sensor history once in every hour, 20 minutes, or 24 hours

**Note:** History includes the humidity, light, motion, and temperature data recorded by the sensor at specified time interval.

- **1-hour**
  - Optional. Displays environmental sensor history once in every 1 (one) hour
- **20-minute**
  - Optional. Displays environmental sensor history once in every 20 minutes
- **24-hour**
  - Optional. Displays environmental sensor history once in every 24 hours

---

**environmental-sensor**

Displays environmental sensor’s recorded data, based on the parameters passed. The system displays the specified recorded data.

**Note:** The environmental sensor records data at the following intervals: 20 minutes, 1 hour, and 24 hours

- **humidity**
  - Displays the minimum, average, and maximum humidity recorded
- **light**
  - Displays the minimum, average, and maximum light recorded
- **motion**
  - Displays the minimum, average, and maximum motion recorded:
- **temperature**
  - Displays the minimum, average, and maximum temperature recorded
- **version**
  - Displays the hardware and firmware versions
- **summary**
  - Displays a summary of the data recorded at following intervals:
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
-----------------------------
<table>
<thead>
<tr>
<th></th>
<th>motion detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>20-minute</td>
<td>0</td>
</tr>
<tr>
<td>1-hour</td>
<td>0</td>
</tr>
<tr>
<td>6-hour</td>
<td>0</td>
</tr>
<tr>
<td>24-hour</td>
<td>0</td>
</tr>
</tbody>
</table>

**temperature-sensor:** Enabled(Demo)
current value: -40.00 deg. C
-----------------------------
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>20-minute</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>1-hour</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>6-hour</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>24-hour</td>
<td>0/0/0</td>
<td></td>
</tr>
</tbody>
</table>

**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
-----------------------------
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>20-minute</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>1-hour</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>6-hour</td>
<td>0/0/0</td>
<td></td>
</tr>
<tr>
<td>24-hour</td>
<td>0/0/0</td>
<td></td>
</tr>
</tbody>
</table>

ap8132-711728#
ap8132-711634# show env-sensor history
Current Time: 2014-11-20 14:08:01 UTC
---------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Sample-Interval</th>
<th>Motion</th>
<th>Temperature</th>
<th>Light</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20-minute</td>
<td>1</td>
<td>64/65/66</td>
<td>77/</td>
</tr>
<tr>
<td>1-hour</td>
<td>24</td>
<td>63/67/70</td>
<td>75/</td>
</tr>
<tr>
<td>6-hour</td>
<td>128</td>
<td>60/62/69</td>
<td>71/</td>
</tr>
<tr>
<td>79</td>
<td>52/56/71</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
---------------------------------------------------------------------------------------
ap8132-711634#

```bash
ap8132-711634#show env-sensor history 20-min
```

<table>
<thead>
<tr>
<th>timestamp</th>
<th>Humidity</th>
<th>Motion</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-07-20 13:51:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 13:53:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 13:55:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 13:57:35 UTC</td>
<td>1</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 13:59:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 14:01:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 14:03:35 UTC</td>
<td>0</td>
<td>64</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 14:05:35 UTC</td>
<td>2</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:07:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:09:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
</tr>
</tbody>
</table>
```

```bash
ap8132-711634#show env-sensor history 1-hr
```

<table>
<thead>
<tr>
<th>timestamp</th>
<th>Humidity</th>
<th>Motion</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-07-20 13:51:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 13:53:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 13:55:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 13:57:35 UTC</td>
<td>1</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 13:59:35 UTC</td>
<td>0</td>
<td>66</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 14:01:35 UTC</td>
<td>0</td>
<td>65</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 14:03:35 UTC</td>
<td>0</td>
<td>64</td>
<td>79</td>
</tr>
<tr>
<td>2014-07-20 14:05:35 UTC</td>
<td>2</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:07:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:09:35 UTC</td>
<td>0</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:42:35 UTC</td>
<td>0</td>
<td>65</td>
<td>81</td>
</tr>
<tr>
<td>2014-07-20 14:43:35 UTC</td>
<td>0</td>
<td>64</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:45:35 UTC</td>
<td>3</td>
<td>66</td>
<td>80</td>
</tr>
<tr>
<td>2014-07-20 14:47:35 UTC</td>
<td>0</td>
<td>66</td>
<td>81</td>
</tr>
</tbody>
</table>
2014-07-20 14:49:35 UTC               0                              66                           80
ap8132-711634#

<DEVICE-NAME>#show env-sensor history 24-hr

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Light</th>
<th>Humidity</th>
<th>Motion</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-07-20 10:10:20 UTC</td>
<td>27</td>
<td>66</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-20 10:30:20 UTC</td>
<td>17</td>
<td>66</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-20 10:50:20 UTC</td>
<td>17</td>
<td>66</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>2014-07-20 11:10:20 UTC</td>
<td>25</td>
<td>66</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>2014-07-20 11:30:20 UTC</td>
<td>24</td>
<td>66</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>2014-07-20 11:50:20 UTC</td>
<td>26</td>
<td>66</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>2014-07-21 08:10:20 UTC</td>
<td>9</td>
<td>65</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-21 08:30:20 UTC</td>
<td>7</td>
<td>65</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-21 08:50:20 UTC</td>
<td>12</td>
<td>65</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-21 09:10:20 UTC</td>
<td>10</td>
<td>65</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-21 09:30:20 UTC</td>
<td>15</td>
<td>65</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>2014-07-21 09:50:20 UTC</td>
<td>19</td>
<td>66</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>
<DEVICE-NAME>#
6.1.17 event-history

Displays event history report

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

- `show event-history {on <DEVICE-OR-DOMAIN-NAME>}`: Displays event history report
  - `on <DEVICE-OR-DOMAIN-NAME>`: Optional. Displays event history report on a device or RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` — Specify the name of the AP, wireless controller, service platform, or RF Domain.

Examples

```
rfs4000-229D58(config)#show event-history
EVENT HISTORY REPORT
Generated on '2014-02-15 15:45:18 UTC' by 'admin'

2014-02-15 15:45:10     rfs4000-229D58  SYSTEM     LOGIN                Successfully
  logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-02-15 15:45:01     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
  'admin' with privilege 'superuser' from '192.168.100.225'
2014-02-15 15:44:37     rfs4000-229D58  SYSTEM     LOGIN                Successfully
  logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-02-15 15:44:16     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
  'admin' with privilege 'superuser' from '192.168.100.225'
2014-02-15 15:12:12     rfs4000-229D58  SYSTEM     LOGOUT               Logged out user
  'admin' with privilege 'superuser' from '192.168.100.224(web)'
2014-02-15 14:44:19     rfs4000-229D58  SYSTEM     CLOCK_RESET          System clock
  reset, Time: 2014-02-15 14:45:30
rfs4000-229D58(config)#
```

```
nx4500-5CFA2B(config)#show event-history
EVENT HISTORY REPORT
Generated on '2014-04-10 14:53:21 UTC' by 'admin'

2014-04-10 14:22:16     nx4500-5CFA2B  SYSTEM     LOGIN                Successfully
  logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-04-10 14:19:39     nx4500-5CFA2B  SYSTEM     LOGOUT               Logged out user
  'admin' with privilege 'superuser' from '192.168.100.222'
2014-04-10 12:45:46     nx4500-5CFA2B  SYSTEM     LOGIN                Successfully
  logged in user 'admin' with privilege 'superuser' from 'ssh'
2014-04-10 12:05:25     nx4500-5CFA2B  DIAG       NEW_LED_STATE        LED state
  message LED_LOCATIONING_OFF from module cfgd
2014-04-10 12:05:24     nx4500-5CFA2B  DIAG       NEW_LED_STATE        LED state
  message LED_LOCATIONING_ON from module cfgd
2014-04-10 12:05:24     nx4500-5CFA2B  SYSTEM     SYSTEM_AUTOUP_ENABLE Autoupgrade enabled for nx45xx
2014-04-10 12:05:23     nx4500-5CFA2B  SYSTEM     SYSTEM_AUTOUP_ENABLE Autoupgrade enabled for nx65xx
2014-04-10 12:05:23     nx4500-5CFA2B  SYSTEM     SYSTEM_AUTOUP_ENABLE Autoupgrade enabled for rfs4000
--More--
nx4500-5CFA2B(config)#
```
6.1.18 event-system-policy

- show commands

Displays detailed event system policy configuration

Supported in the following platforms:

- Access Points — AP300, 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, 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

<table>
<thead>
<tr>
<th>MODULE</th>
<th>EVENT</th>
<th>SYSLOG</th>
<th>SNMP</th>
<th>FORWARD</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>radius-discon-msg</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>default</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#
6.1.19 file

- **show commands**

Displays file system information

---

**NOTE:** This command is not available in the USER EXEC mode.

---

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`show file [information <FILE>|systems]`

**Parameters**

- **show file [information <FILE>|systems]**

<table>
<thead>
<tr>
<th>information &lt;FILE&gt;</th>
<th>Displays file information</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FILE&gt;</td>
<td>&lt;FILE&gt; – Specify the file name.</td>
</tr>
</tbody>
</table>

| systems            | Lists all file systems present in the system |

**Examples**

```
rfs7000-37FABE(config)#show file systems
File Systems:

<table>
<thead>
<tr>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Type</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>system:</td>
</tr>
<tr>
<td>10485760</td>
<td>9916416</td>
<td>flash</td>
<td>nvram:</td>
</tr>
<tr>
<td>20971520</td>
<td>20131840</td>
<td>flash</td>
<td>flash:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>(null)</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rdp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>sftp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>http:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>ftp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>tftp:</td>
</tr>
<tr>
<td>20971520</td>
<td>20131840</td>
<td></td>
<td>hotspot:</td>
</tr>
</tbody>
</table>
```

```
rfs7000-37FABE(config)#
```
### 6.1.20 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

- `show firewall [dhcp|dos|flows]`
- `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|igmp|ip|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}`
- `show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}|wireless-client <MAC>|on <DEVICE-NAME>}`

**Parameters**
- `show firewall [dhcp snoop-table|dos stats] {on <DEVICE-NAME>}`

| 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|igmp|ip|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

<table>
<thead>
<tr>
<th>dir</th>
<th>wired-wired</th>
<th>wired-wireless</th>
<th>wireless-wired</th>
<th>wireless-wireless</th>
</tr>
</thead>
</table>
|     | Optional. Matches the packet flow direction
|     | 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</td>
<td>Optional. Matches the destination port with the specified port</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>• port &lt;1-65535&gt; – Specifies the destination port number from 1 - 65535</td>
</tr>
<tr>
<td>ether</td>
<td>Optional. Displays Ethernet filter options</td>
</tr>
<tr>
<td>[dst &lt;MAC&gt;</td>
<td>• dst &lt;MAC&gt; – Matches only the destination MAC address</td>
</tr>
<tr>
<td>host &lt;MAC&gt;</td>
<td>• host &lt;MAC&gt; – Matches flows containing the specified MAC address</td>
</tr>
<tr>
<td>src &lt;MAC&gt;</td>
<td>• src &lt;MAC&gt; – Matches only the source MAC address</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>• 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</td>
<td>Optional. Matches the traffic flow type</td>
</tr>
<tr>
<td>[bridged</td>
<td>• bridged – Bridged flows</td>
</tr>
<tr>
<td>natted</td>
<td>• natted – Natted flows</td>
</tr>
<tr>
<td>routed</td>
<td>• routed – Routed flows</td>
</tr>
<tr>
<td>wired</td>
<td>• wired – Flows belonging to wired hosts</td>
</tr>
<tr>
<td>wireless</td>
<td>• wireless – Flows containing a mobile unit</td>
</tr>
<tr>
<td>icmp {code</td>
<td>type}</td>
</tr>
<tr>
<td>ip [dst &lt;IP&gt;</td>
<td>• code – Matches flows with the specified ICMP code</td>
</tr>
<tr>
<td>host &lt;IP&gt;</td>
<td>• type – Matches flows with the specified ICMP type</td>
</tr>
<tr>
<td>proto &lt;0-254&gt;</td>
<td></td>
</tr>
<tr>
<td>src &lt;IP&gt;</td>
<td></td>
</tr>
<tr>
<td>max-idle</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>&lt;1-4294967295&gt;</td>
<td></td>
</tr>
<tr>
<td>min-bytes</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>&lt;1-4294967295&gt;</td>
<td></td>
</tr>
<tr>
<td>min-idle</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>&lt;1-4294967295&gt;</td>
<td></td>
</tr>
<tr>
<td>min-pkts</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>&lt;1-4294967295&gt;</td>
<td></td>
</tr>
<tr>
<td>not</td>
<td>Optional. Negates the filter expression selected</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Matches either the source or destination port. Specify a port from 1 - 65535.</td>
</tr>
<tr>
<td>src &lt;1-65535&gt;</td>
<td>Optional. Matches only the source port with the specified port. Specify a port from 1 - 65535.</td>
</tr>
<tr>
<td>tcp</td>
<td>Optional. Matches TCP flows</td>
</tr>
<tr>
<td>udp</td>
<td>Optional. Matches UDP flows</td>
</tr>
</tbody>
</table>
- `show firewall flows {management {on <DEVICE-NAME>}}/stats {on <DEVICE-NAME>}}/wireless-client <MAC>{on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>firewall flows</th>
<th>Notifies a session has been established</th>
</tr>
</thead>
<tbody>
<tr>
<td>management</td>
<td>Optional. Displays management traffic firewall flows</td>
</tr>
<tr>
<td><code>{on &lt;DEVICE-NAME&gt;}</code></td>
<td>- Optional. Displays firewall flows 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>stats</td>
<td>Optional. Displays active session summary</td>
</tr>
<tr>
<td><code>{on &lt;DEVICE-NAME&gt;}</code></td>
<td>- Optional. Displays active session summary 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>wireless-client</td>
<td>Optional. Displays wireless clients firewall flows</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>- <code>&lt;MAC&gt;</code> – Specify the MAC address of the wireless client.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays all firewall flows 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**

```
rfs7000-37FABE(config)#show firewall dhcp snoop-table
Snoop Binding <157.235.208.252, 00-15-70-37-FA-BE, Vlan 4>
Type Controller-SVI, Touched 32 seconds ago
Snoop Binding <172.16.10.2, 00-15-70-37-FA-BE, Vlan 1>
Type Controller-SVI, Touched 1 seconds ago
```

```
rfs7000-37FABE(config)#show firewall flows management
========== Flow# 1 Summary ==========
Forward:
Vlan 1, TCP 172.16.10.10 port 3995 > 172.16.10.1 port 22
00-02-B3-28-D1-55 > 00-15-70-37-FA-BE, ingress port ge1
Egress port: <local>, Egress interface: vlan1, Next hop: <local> (00-15-70-37-FA-BE)
573 packets, 49202 bytes, last packet 0 seconds ago
Reverse:
Vlan 1, TCP 172.16.10.1 port 22 > 172.16.10.10 port 3995
00-15-70-37-FA-BE > 00-02-B3-28-D1-55, ingress port local
Egress port: gel, Egress interface: vlan1, Next hop: 172.16.10.10 (00-02-B3-28-D1-55)
552 packets, 63541 bytes, last packet 0 seconds ago
TCP state: Established
Flow times out in 1 hour 30 minutes
```

```
rfs7000-37FABE(config)#show firewall flows stats
Active Flows 2
TCP flows 1
UDP flows 0
DHCP flows 1
ICMP flows 0
IPsec flows 0
L3/Unknown flows 0
```

```
rfs7000-37FABE(config)#
```
## 6.1.21 global

- **show commands**

Displays global information for network devices based on the parameters passed.

**Supported in the following platforms:**
- Access Points — AP300, 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, 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>
</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 [&lt;DOMAIN-NAME&gt;</td>
<td>not &lt;DOMAIN-NAME&gt;]</td>
</tr>
</tbody>
</table>

- **show global domain managers**

| global domain managers | Displays global information for all RF Domains and managers in the network |
Examples

rfs4000-229D58#show global device-list
--------------------------------------------
<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>00-23-68-22-9D-58</td>
<td>rfs4000-229D58</td>
<td>rfs4000</td>
<td></td>
<td>default</td>
<td></td>
<td>online</td>
</tr>
</tbody>
</table>
--------------------------------------------
Total number of clients displayed: 1
rfs4000-229D58#

rfs4000-229D58#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>00-23-68-22-9D-58</td>
<td>rfs4000-229D58</td>
<td>rfs4000</td>
<td></td>
<td>default</td>
<td></td>
<td>online</td>
</tr>
</tbody>
</table>
--------------------------------------------
Total number of clients displayed: 1
rfs4000-229D58#

rfs4000-229D58#show global domain managers
------------------------------------------
<table>
<thead>
<tr>
<th>RF-DOMAIN</th>
<th>MANAGER</th>
<th>HOST-NAME</th>
<th>APS CLIENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>00-23-68-22-9D-58</td>
<td>rfs4000-229D58</td>
<td>1 0</td>
</tr>
</tbody>
</table>
------------------------------------------
Total number of RF-domain displayed: 1
rfs4000-229D58#
6.1.22 `gre`

Displays GRE tunnel info

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show gre info
```

Parameters

- `show gre info`

Examples

```
nx4500-5CFA2B>show gre info
Gre Tunnel info:
    {'No tunnel found': 0}
nx4500-5CFA2B>
```
### 6.1.23 interface

> **show commands**

Displays configured system interfaces and their status.

**Supported in the following platforms:**
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|on|port-channel <1-2>|pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}
```

**Parameters**

- **interfaces** Optional. Displays system interface status based on the parameters passed
  - `<INTERFACE-NAME>` Optional. Displays status of 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
    - `<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
  - **switch port** 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 are the interfaces available on a RFS7000 controller:

```
rfs7000-37FABE(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
pppoel        PPP Over Ethernet interface
switchport    Status of Layer2 interfaces
vlan          Switch VLAN interface
wwan1         Wireless WAN interface
|             Output modifiers
>             Output redirection
>>            Output redirection appending
<r>
```

```
rfs7000-37FABE(config)#
```

Following are the interfaces available on a NX45XX and NX65XX series service platform:

```
xn4500-5CFA2B(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
pppoel        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
<r>
```

```
xn4500-5CFA2B(config)#
```

```
rfs7000-37FABE(config)#show interface switchport
---------------------------------------------------------------------------------------
INTERFACE          STATUS   MODE     VLAN(S)
---------------------------------------------------------------------------------------
ge1                UP       access   1
ge2                UP       access   1
ge3                UP       access   1
ge4                UP       access   1
---------------------------------------------------------------------------------------
A '*' next to the VLAN ID indicates the native vlan for that trunk port
```

```
rfs7000-37FABE(config)#
```

```
rfs7000-37FABE(config)#show interface vlan 1
Interface vlan1 is UP
Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
Index: 4, Metric: 1, MTU: 1500
IP-Address: 172.16.10.1/24
    input packets 587971, bytes 58545041, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 56223, bytes 4995566, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

```
rfs7000-37FABE(config)#
```
rfs7000-37FABE(config)# show interface ge 2
Interface ge2 is DOWN
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-37-FA-C0
  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 broadcast, 0 multicast
    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

rfs7000-37FABE(config)#

rfs7000-37FABE(config)# show interface counters

<table>
<thead>
<tr>
<th>#</th>
<th>MAC</th>
<th>RX-PKTS</th>
<th>RX-BYTES</th>
<th>RX-DROP</th>
<th>TX-PKTS</th>
<th>TX-BYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX-DROP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>me1</td>
<td>00-....-F7 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan1</td>
<td>00-....-BE 353854</td>
<td>57627570</td>
<td>0</td>
<td>126392</td>
<td>37379394</td>
<td>0</td>
</tr>
<tr>
<td>ge1</td>
<td>00-....-BF 299841</td>
<td>32267476</td>
<td>0</td>
<td>117557</td>
<td>41052744</td>
<td>0</td>
</tr>
<tr>
<td>ge2</td>
<td>00-....-C0 0</td>
<td>0</td>
<td>0</td>
<td>274490</td>
<td>30705325</td>
<td>0</td>
</tr>
<tr>
<td>ge3</td>
<td>00-....-C1 0</td>
<td>0</td>
<td>0</td>
<td>274490</td>
<td>30705325</td>
<td>0</td>
</tr>
<tr>
<td>ge4</td>
<td>00-....-C2 0</td>
<td>0</td>
<td>0</td>
<td>274490</td>
<td>30705325</td>
<td>0</td>
</tr>
</tbody>
</table>

rfs7000-37FABE(config)#

nx6500-31FABE(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 1</td>
<td>1</td>
</tr>
<tr>
<td>ge2</td>
<td>DOWN</td>
<td>access 1</td>
<td></td>
</tr>
</tbody>
</table>

A '*' next to the VLAN ID indicates the native vlan for that trunk port

nx6500-31FABE(config)#

nx6500-31FABE(config)# show interface vlan 1
Interface vlan1 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 4, Metric: 1, MTU: 1500
  IP-Address: 172.16.10.1/24
    input packets 587971, bytes 58545041, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 56223, bytes 4995566, dropped 0
    output errors 0, abort 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

nx6500-31FABE(config)#
nx6500-31FABE(config)#show interface ge 2
Interface ge2 is DOWN
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-37-FA-C0
  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 broadcast, 0 multicast
    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

nx6500-31FABE(config)#

nx6500-31FABE(config)#show interface counters

<table>
<thead>
<tr>
<th>#</th>
<th>MAC</th>
<th>RX-PKTS</th>
<th>RX-BYTES</th>
<th>RX-DROP</th>
<th>TX-PKTS</th>
<th>TX-BYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX-DROP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan1</td>
<td>00-...-BE 588384</td>
<td>58580154</td>
<td>0</td>
<td>56435</td>
<td>5013682</td>
<td>0</td>
</tr>
<tr>
<td>ge1</td>
<td>00-...-BF 1906950</td>
<td>175560930</td>
<td>0</td>
<td>1402226</td>
<td>589235764</td>
<td>0</td>
</tr>
<tr>
<td>ge2</td>
<td>00-...-C0 0</td>
<td>0</td>
<td>0</td>
<td>501615</td>
<td>60939303</td>
<td>0</td>
</tr>
</tbody>
</table>

nx6500-31FABE(config)#
### 6.1.24 ip

#### show commands

Displays IP related information

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
show ip [arp|ddns|default-gateways|dhcp|dhcp-vendor-options|domain-name|igmp|interface|name-server|nat|ospf|route|routing]
show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}
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 igmp snooping [mrouter|vlan]
show ip igmp snooping mrouter vlan <1-4095> {on <DEVICE-NAME>}
show ip igmp snooping vlan <1-4095> {<IP>} {(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|pppoe1|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</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>on &lt;DEVICE-NAME&gt;</td>
<td>The following keyword is recursive and common to the 'vlan-name' parameter:</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-NAME&gt; — Optional. Displays ARP configuration 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 ip ddns bindings {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ddns bindings</td>
<td>Displays Dynamic Domain Name Server (DDNS) configuration details</td>
</tr>
<tr>
<td>bindings</td>
<td>Displays DDNS address bindings</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>• &lt;DEVICE-NAME&gt; – Optional. Displays 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>

### show ip dhcp [networks|status] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp</td>
<td>Displays DHCP server related details, such as network and status</td>
</tr>
<tr>
<td>networks</td>
<td>Displays DHCP server network details</td>
</tr>
<tr>
<td>status</td>
<td>Displays DHCP server status</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keyword is common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Optional. Displays server status and network 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 ip dhcp binding {manual} {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp binding</td>
<td>Displays the DHCP server configuration details</td>
</tr>
<tr>
<td>bindings</td>
<td>Displays DHCP address bindings</td>
</tr>
<tr>
<td>manual</td>
<td>Displays static DHCP address bindings</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keyword is recursive and common to the 'manual' parameter:</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Optional. Displays DHCP 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>

### show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip default-gateways</td>
<td>Displays all learnt default gateways</td>
</tr>
<tr>
<td>ip dhcp-vendor-options</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>ip domain-name</td>
<td>Displays the DNS default domain</td>
</tr>
<tr>
<td>ip name-server</td>
<td>Displays the DNS name server details</td>
</tr>
<tr>
<td>ip routing</td>
<td>Displays routing status</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>• &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>

### show ip igmp snooping mrouter vlan <1-4095> {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>Displays the IGMP snooping configuration</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>mrouter</td>
<td>Displays the IGMP snooping multicast router (mrouter) configuration</td>
</tr>
</tbody>
</table>
| `show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}` | Displays the IGMP snooping multicast router configuration for a VLAN  
- `<1-4095>` – Specify the VLAN ID from 1 - 4095.  
- `on <DEVICE-NAME>` – Optional. Displays the IGMP snooping mrouter configuration on a specified device  
- `<DEVICE-NAME>` – Specify the name of the AP or wireless controller. |
| `show ip interface {<INTERFACE-NAME>|brief} {(on <DEVICE-NAME>)}` | Displays the IGMP snooping configuration  
- `<INTERFACE-NAME>` – Displays a specified interface status. Specify the interface name.  
- `brief` – Displays a brief summary of all interface status and configuration  
- `on <DEVICE-NAME>` – Optional. Displays configuration details on a specified device  
- `<DEVICE-NAME>` – Specify the name of the AP or wireless controller. |
| `show ip nat translations verbose {on <DEVICE-NAME>}` | Displays Network Address Translation (NAT) translations  
- `verbose` – Displays detailed NAT translations  
- `on <DEVICE-NAME>` – Optional. Displays NAT translations on a specified device  
- `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform. |
| `show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|pppoe1|wwan1} {(on <DEVICE-NAME>)}` | 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. |
show ip ospf

On <DEVICE-NAME>

Example:

```
show ip arp
```

```
+---------+----------------+-----------------+--------+
| IP      | MAC            | INTERFACE       | TYPE   |
|---------+----------------+-----------------+--------+
| 172.16.10.12 | 5C-D9-98-4C-04-51 | vlan1           | dynamic|
| 172.16.10.4  | 00-15-70-38-06-49 | vlan1           | dynamic|
```

```
show ip interface brief
```

```
+---------+-----------------+--------+-------+-------+
| INTERFACE| IP-ADDRESS/MASK | TYPE   | STATUS| PROTOCOL|
|----------+-----------------+--------+-------+----------+
| me1      | 192.168.0.1/24  | primary| UP    | down     |
| vlan1    | 172.16.10.1/24  | primary| UP    | up       |
```
rfs7000-37FABE(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

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route pc

<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>172.16.10.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway

rfs7000-37FABE(config)#

rfs7000-37FABE(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>172.16.10.0/24</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

rfs7000-37FABE(config)#

rfs7000-37FABE(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

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip routing

IP routing is enabled.

rfs7000-37FABE(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(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>172.16.10.0/24</td>
<td>direct</td>
<td>C</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Flags:  C - Connected  G - Gateway  O - OSPF  S - Static

rfs7000-37FABE#
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>192.168.0.0/24</td>
<td>direct</td>
<td>C</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

rfs4000-882A17#

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)#

nx6500-31FABE(config)#show ip routing
IP routing is enabled.

nx6500-31FABE(config)#

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>
6.1.25 ip-access-list

Displays IP access list statistics

NOTE: This command is not available in the USER EXEC Mode.

Supported in the following platforms:
- Access Points — AP300, 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, 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 <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` 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>` – Optional. 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 2Hitcount: 0
   permit ip host 200.200.200.99 any rule-precedence 3Hitcount: 0

rfs4000-229D58#
```

```
x6524-5483B0#show ip-access-list stats scaleacl | i 125
   permit ip host 125.1.1.1 any rule-precedence 125Hitcount: 893Hardware
Hitcount: 3120
   permit ip host 125.2.1.1 any rule-precedence 346Hitcount: 0Hardware
Hitcount: 0
x6524-5483B0#
```
6.1.26 l2tpv3

> show commands

Displays a Layer 2 Tunnel Protocol Version 3 (L2TPV3) session information

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

\[
\text{l2tpv3} \{ \text{on/tunnel/tunnel-summary} \} \\
\text{l2tpv3} \{ \text{on <DEVICE-NAME>} \} \\
\text{l2tpv3} \{ \text{tunnel <L2TPV3-TUNNEL-NAME>} \} \{ \text{session <L2TPV3-SESSION-NAME>} \} \\
\{ \text{on <DEVICE-NAME>} \} \\
\text{l2tpv3} \{ \text{tunnel-summary} \} \{ \text{down/on/up} \} \\
\text{l2tpv3} \{ \text{tunnel-summary} \} \{ \text{on <DEVICE-NAME>} \} \\
\text{l2tpv3} \{ \text{tunnel-summary} \} \{ \text{down/on/up} \} \{ \text{on <DEVICE-NAME>} \}
\]

Parameters
- l2tpv3 \{ \text{on <DEVICE-NAME>} \}

<table>
<thead>
<tr>
<th>l2tpv3 { on &lt;DEVICE-NAME&gt; }</th>
<th>Displays a L2TPv3 tunnel and session details or summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ on &lt;DEVICE-NAME&gt; }</td>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Displays L2TPv3 information on a specified access point or wireless controller</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-NAME&gt; – Specify the name of AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- l2tpv3 \{ tunnel <L2TPV3-TUNNEL-NAME> \} \{ session <L2TPV3-SESSION-NAME> \} \{ on <DEVICE-NAME> \}

<table>
<thead>
<tr>
<th>l2tpv3 { tunnel &lt;L2TPV3-TUNNEL-NAME&gt; } { session &lt;L2TPV3-SESSION-NAME&gt; } { on &lt;DEVICE-NAME&gt; }</th>
<th>Displays a L2TPv3 tunnel and session details or summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel &lt;L2TPV3-TUNNEL-NAME&gt;</td>
<td>Optional. Displays a specified L2TPv3 tunnel information</td>
</tr>
<tr>
<td></td>
<td>- &lt;L2TPV3-TUNNEL-NAME&gt; – Specify the L2TPv3 tunnel name.</td>
</tr>
<tr>
<td>session &lt;L2TPV3-SESSION-NAME&gt;</td>
<td>Optional. Displays a specified L2TPv3 tunnel session information</td>
</tr>
<tr>
<td></td>
<td>- &lt;L2TPV3-SESSION-NAME&gt; – Specify the session name.</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keyword is recursive and common to the ‘session &lt;L2TPV3-SESSION-NAME&gt;’ parameter.</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Displays a L2TPv3 tunnel and session details, based on the parameters passed, on a specified device.</td>
</tr>
<tr>
<td></td>
<td>- &lt;DEVICE-NAME&gt; – Specify the name of AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>


- **l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}**

  **l2tpv3**
  Displays L2TPv3 tunnel and session details or summary

  **Note:** For an L2TPv3 tunnel over Auto IPSec, the tunnel status is displayed as: Established (secured by ipsec)

  **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.

- **l2tpv3 {tunnel-summary} {down|up} {on <DEVICE-NAME>}**

  **l2tpv3**
  Displays a L2TPv3 tunnel and session details or summary

  **tunnel-summary**
  Optional. Displays a L2TPv3 tunnel summary, based on the parameters passed

  **down**
  Optional. Displays un-established tunnels summary

  **up**
  Optional. Displays established tunnels summary

  **on <DEVICE-NAME>**
  The following keyword is common to the 'down' and 'up' parameters:

  - on <DEVICE-NAME> – Optional. Displays summary, for un-established or established tunnels, on a specified device
  - <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

**Examples**

ap7131-11E6C4#show l2tpv3 tunnel-summary

---

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Tunnel Name</th>
<th>Tunnel State</th>
<th>Estd/Total Sessions</th>
<th>Encapsulation Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>testTunnel</td>
<td>Established</td>
<td>1/1</td>
<td>IP</td>
</tr>
</tbody>
</table>

Total Number of Tunnels 1

ap7131-11E6C4#

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 : 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#
6.1.27 ldap-agent

Displays an LDAP agent's join status (join status to a LDAP server domain)

NOTE: This command is not available in the USER EXEC Mode.

Supported in the following platforms:
- Access Points — AP300, AP622, AP650, ES6510, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
show ldap-agent join-status {on <DEVICE-NAME>}

Parameters
- show ldap-agent join-status {on <DEVICE-NAME>}

Examples
rfs6000-81701D#sh 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#
### 6.1.28 licenses

- **show commands**

Displays installed licenses and usage information

Supported in the following platforms:

- **Access Points** — AP300, 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, NX7522, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show licenses {borrowed|lent}
```

**Parameters**

- **show licenses {borrowed|lent}**

| 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 : 41a5a30ee9bb0bd78e943dba0a36ac34d3cdc66c956ef1f449d89fc8beb032ac9747a8f0c9f98f
    Value  : 1
  AAP-LICENSE
    String : 41a5a30ee9bb0bd7f8d421c001f7c9cb3c66c956ef1f41960aa2a030abb4ac9747a8f0c9f98f
    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>0</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.

```bash
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(HRS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-15-70-37-FA-BE</td>
<td>rfs7000-37FABE</td>
<td>AP</td>
<td>1</td>
<td>00-00-00-04-0A-01</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>00-00-00-04-0A-01</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>00-00-00-04-0A-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>1</td>
<td>00-00-00-04-0A-0D</td>
<td>rfs4000-04040D</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>00-15-70-81-70-1D</td>
<td>rfs6000-81701D</td>
<td>AP</td>
<td>1</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-FA-BE</td>
<td>rfs7000-37FABE</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>

rfs4000-881E4B#
### 6.1.29 lldp

> **show commands**

Displays *Link Layer Discovery Protocol (LLDP)* information

Supported in the following platforms:

- **Access Points** — AP300, 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, 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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp</td>
<td>Displays an LLDP neighbors table or aggregated LLDP neighbors table</td>
</tr>
<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></td>
<td>• &lt;DEVICE-NAME&gt; — Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
</tbody>
</table>

- **show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>))**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp</td>
<td>Displays an LLDP neighbors table or aggregated LLDP neighbors table</td>
</tr>
<tr>
<td>report</td>
<td>Displays an aggregated LLDP neighbors table</td>
</tr>
<tr>
<td>detail</td>
<td>• detail — Optional. Displays detailed aggregated LLDP neighbors table</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keyword is recursive and common to the ‘report detail’ parameter:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; — Displays an aggregated LLDP neighbors table 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(config)#show lldp neighbors
rfs7000-37FABE(config) #

rfs7000-37FABE(config)#show lldp neighbors
rfs7000-37FABE(config) #
```
6.1.30 logging

Displays the network’s activity log

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

show logging {on <DEVICE-NAME>}

Parameters

- show logging {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Logging module {on &lt;DEVICE-NAME&gt;}</th>
<th>Displays logging information on a specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DEVICE-NAME&gt; – Optional. Specify the name of the AP, wireless controller, or service platform.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config)#show logging

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

Log Buffer (359 bytes):

Jan 23 19:50:40 2014: rfs4000-229D58 : %SYSTEM-3-LOGIN_FAIL: Log-in failed for user 'admin' from 'ssh'
Jan 22 00:04:14 2014: rfs4000-229D58 : %SYSTEM-3-UI_USER_AUTH_FAIL: UI user 'Admin' from: '192.168.13.10' authentication failed
rfs4000-229D58(config)#
6.1.31 mac-access-list-stats

- show commands

Displays MAC access list statistics

NOTE: This command is not present in USER EXEC mode.

Supported in the following platforms:
- Access Points — AP300, 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, 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}  
- <MAC-ACCESS-LIST> Optional. Displays statistics for a specified MAC access list. Specify the MAC access list name.
- on <DEVICE-NAME> Optional. Displays all or a specified MAC access list statistics on a specified device
  - <DEVICE-NAME> — Specify the name of the AP, wireless controller, or service platform.

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#
6.1.32 mac-address-table

- **show commands**

Displays MAC address table entries

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show mac-address-table [on <DEVICE-NAME>]
```

**Parameters**

- **on <DEVICE-NAME>** – Optional. Displays MAC address table entries on a specified device

  - `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

**Examples**

```
rfs7000-37FABE(config)#show mac-address-table
--------------------------------------------------------
BRIDGE VLAN PORT     MAC               STATE
--------------------------------------------------------
1      1    ge1              00-02-B3-28-D1-55 forward
1      1    ge1              00-23-68-11-E6-C4 forward
1      1    ge1              00-A0-F8-68-D5-66 forward
1      1    ge1              5C-D9-98-4C-04-51 forward
--------------------------------------------------------
Total number of MACs displayed: 4
rfs7000-37FABE(config)#
```
### 6.1.33 macauth

*show commands*

Displays details of wired ports that have MAC address authentication enabled.

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 macauth [all | interface | on]
```

```
show macauth [all | interface [INTERFACE-NAME] | ge <1-5> | port-channel <1-3> | up1] {on <DEVICE-NAME>}
```

#### Parameters
- **show macauth [all | interface [INTERFACE-NAME] | ge <1-5> | port-channel <1-3> | up1] {on <DEVICE-NAME>}
- **show macauth [all | interface [INTERFACE-NAME] | ge <1-5> | port-channel <1-3> | up1] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>macauth</th>
<th>Displays MAC authentication related information for all interfaces or all interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays MAC authentication related information for all interfaces</td>
</tr>
<tr>
<td>interface</td>
<td>Displays MAC authentication related information for a specified interface. Specify the interface using one of the following options:</td>
</tr>
<tr>
<td>&lt;INTERFACE-NAME&gt;</td>
<td>- &lt;INTERFACE-NAME&gt; – Selects the interface identified by the &lt;INTERFACE-NAME&gt; keyword</td>
</tr>
<tr>
<td>ge &lt;1-5&gt;</td>
<td>- ge &lt;1-5&gt; – Selects the GigabitEthernet interface identified by the index number</td>
</tr>
<tr>
<td>port-channel &lt;1-3&gt;</td>
<td>- port-channel &lt;1-3&gt; – Selects the port channel interface identified by the index number</td>
</tr>
<tr>
<td>up1</td>
<td>- up1 – Selects the WAN Ethernet interface</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to the ‘all’ and ‘interface’ parameters:</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Displays MAC authentication related 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

```
rfs4000-229D58(config)#show macauth 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)#
6.1.34 mint

- **show commands** Displays MiNT protocol configuration commands

Supported in the following platforms:
  - Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
show mint [config|dis|id|info|known-adopters|links|lsp|lsp-db|mlcp|neighbors|route|stats|tunnel-controller|tunneled-vlans]
```

```plaintext
show mint [config|id|info|known-adopters|route|stats|tunnel-controller|tunneled-vlans]
  {on <DEVICE-NAME>}
```

```plaintext
show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}
```

```plaintext
show mint lsp
```

```plaintext
show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}
```

```plaintext
show mint mlcp {history} {(on <DEVICE-NAME>)}
```

**Parameters**

- **show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on <DEVICE-NAME>}**

<table>
<thead>
<tr>
<th>mint</th>
<th>Displays MiNT protocol information based on the parameters passed</th>
</tr>
</thead>
<tbody>
<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>- <code>on &lt;DEVICE-NAME&gt;</code> — Optional. Displays MiNT protocol details 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>

```plaintext
- show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}
```

<table>
<thead>
<tr>
<th>mint</th>
<th>Displays MiNT protocol information based on the parameters passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>dis</td>
<td>Displays MiNT network Designated Intermediate Systems (DISes) and 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</code></td>
<td>Displays MiNT protocol information based on the parameters passed</td>
</tr>
<tr>
<td><code>lsp</code></td>
<td>Displays this router’s MiNT Label Switched Paths (LSPs)</td>
</tr>
<tr>
<td><code>show mint lsp-db</code></td>
<td>Displays MiNT LSP database entries</td>
</tr>
<tr>
<td><code>lsp-db</code></td>
<td>Displays MiNT LSP database entries</td>
</tr>
<tr>
<td><code>show mint mlcp</code></td>
<td>Displays MiNT Link Creation Protocol (MLCP) status</td>
</tr>
<tr>
<td><code>mlcp</code></td>
<td>Displays MiNT Link Creation Protocol (MLCP) status</td>
</tr>
<tr>
<td><code>history</code></td>
<td>Displays MLCP client history</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
```

- `tunnel-controller` Displays details of MiNT VLAN network tunnel wireless controllers for extended VLAN load balancing
- `details {on <DEVICE-NAME>}` The following keywords are common to the ‘dis’, ‘links’, ‘neighbors’, and ‘tunnel-controller’ parameters:
  - `details` – Optional. Displays detailed MiNT information
  - `on <DEVICE-NAME>` – Optional. This is a recursive parameter, which displays MiNT information on a specified device
- `on <DEVICE-NAME>` Displays MiNT LSP database entries on a specified device
- `on <DEVICE-NAME>` Displays MLCP client history on a specified device
- `<DEVICE-NAME>` Specify the name of the AP or wireless controller
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)#

rfs7000-37FABE(config)#show mint route
Destination : Next-Hop(s)
70.37.FA.BE : 70.37.FA.BE via self
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show mint known-adopters
70.37.FA.BE
rfs7000-37FABE(config)#

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
rfs7000-37FABE(config)#

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#
6.1.35 ntp

Displays *Network Time Protocol* (NTP) information. NTP enables clock synchronization within a network.

Supported in the following platforms:
- **Access Points** — AP300, 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, 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  
|-------------------------------|----------------------------------|
|                               | • detail — Optional. Displays detailed NTP associations  
|                               | • on <DEVICE-NAME> — Optional. Displays NTP associations on a specified device  
|                               | • <DEVICE-NAME> — Specify the name of the AP, wireless controller, or service platform.  

| ntp status {on <DEVICE-NAME>} | Displays NTP association status  
|---------------------------------|---------------------------------|
|                                 | • on <DEVICE-NAME> — Optional. Displays NTP association status on a specified device  
|                                 | • <DEVICE-NAME> — Specify the name of the AP, wireless controller, or service platform.  

**Examples**

```
rfs7000-37FABE> show ntp associations
  address    ref clock    st when poll reach delay offset  disp
  * master (synced), # master (unsynced), + selected, - candidate, ~ configured

rfs7000-37FABE> show ntp status
  Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is 2**0
  reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
  clock offset is 0.000 msec, root delay is 0.000 msec
  root dispersion is 0.000 msec

rfs7000-37FABE>  
```
### 6.1.36 password-encryption

Displays password encryption status (enabled/disabled)

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
show password-encryption status
```

**Parameters**
- `show password-encryption status`

**Examples**
```
rfs7000-37FABE(config)#show password-encryption status
Password encryption is disabled
rfs7000-37FABE(config)#
```
6.1.37 power

Displays Power over Ethernet (PoE) information

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

```
show power [configuration|status] {on <DEVICE-NAME>}
```

Parameters

- `configuration` {on <DEVICE-NAME>}
  - Displays detailed PoE configuration
  - `<DEVICE-NAME>` — Specify the name of the AP, wireless controller, or service platform.

- `status` {on <DEVICE-NAME>}
  - Displays PoE status
  - `<DEVICE-NAME>` — Specify the name of the AP, wireless controller, or service platform.

Examples

```
nx6500-31FABE(config)#show power status
System Voltage: 53.4 volts
Guard Band: 32 watts
Power Budget: 190 watts Power Consumption: 0 watts
poe device 1 temperature 35C
poe device 2 temperature 38C

<table>
<thead>
<tr>
<th>PORT</th>
<th>VOLTS</th>
<th>mA</th>
<th>WATTS</th>
<th>CLASS</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge1</td>
<td>0.0</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>Off</td>
</tr>
<tr>
<td>ge2</td>
<td>0.0</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>Off</td>
</tr>
</tbody>
</table>

nx6500-31FABE(config)#
```

```
NX6500-37FAAA(config)#show power configuration

<table>
<thead>
<tr>
<th>PORT</th>
<th>PRIORITY</th>
<th>POWER LIMIT</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge1</td>
<td>low</td>
<td>30.0W</td>
<td>yes</td>
</tr>
<tr>
<td>ge2</td>
<td>low</td>
<td>30.0W</td>
<td>yes</td>
</tr>
</tbody>
</table>

NX6500-37FAAA(config)#
```

```
rfs4000-88E4B#show power configuration on ap7502-746801
Port fe3 power enable: Yes
Port fe3 power best-effort enable: Yes

rfs4000-88E4B#show power status on ap7502-746801
PoE in: 802.3at Class 4
Port fe3 status: On
```
**6.1.38 pppoe-client**

 Displays Point-to-Point Protocol over Ethernet (PPPoE) client information

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

**Parameters**
- show pppoe-client [configuration|status] {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe-client</td>
<td>Displays PPPoE client information (configuration and status)</td>
</tr>
<tr>
<td>configuration</td>
<td>Displays detailed PPPoE client configuration</td>
</tr>
<tr>
<td>status</td>
<td>Displays detailed PPPoE client status</td>
</tr>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>The following keywords are common to 'configuration' and 'status' parameters:</td>
</tr>
<tr>
<td></td>
<td>- on &lt;DEVICE-NAME&gt; – Optional. Displays detailed PPPoE client status or configuration 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(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)#
```
6.1.39 privilege

Displays a device's existing privilege level

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show privilege
```

Parameters

None

Examples

```
rfs7000-37FABE(config)#show privilege
Current user privilege: superuser
rfs7000-37FABE(config)#
```
6.1.40 reload

Displays scheduled reload information for a specific device

**NOTE:** This command is not present in the USER EXEC mode.

Supported in the following platforms:
- **Access Points** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**
- `show reload {on <DEVICE-OR-DOMAIN-NAME>}`

**Examples**

```
rfs7000-37FABE(config)#show reload
No reload is scheduled.
rfs7000-37FABE(config)#
```
### 6.1.41 rf-domain-manager

- **show commands**

Displays RF Domain manager selection details

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show rf-domain-manager [on <DEVICE-OR-DOMAIN-NAME>]
```

**Parameters**

- **show rf-domain-manager [on <DEVICE-OR-DOMAIN-NAME>]**
  - rf-domain-manager Displays RF Domain manager selection details
  - on <DEVICE-OR-DOMAIN-NAME> Optional. Displays RF Domain manager selection details on a specified device or domain
  - <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)#
```
6.1.42 role

- **show commands**
  Displays role based firewall information

Supported in the following platforms:
- **Access Points** — AP300, 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, 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></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays LDAP server status on a specified device</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>role wireless-clients</th>
<th>Displays clients associated with roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays clients associated with roles on a specified device</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config)#show role wireless-client
No ROLE statistics found.
rfs7000-37FABE(config)#
```
6.1.43 route-maps

Displays route map statistics for defined device routes

Supported in the following platforms:

- Access Points — AP300, 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, 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>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays route map 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>

Note: For more information on route maps, see route-map on page 25-5.

Examples

rfs7000-37FABE(config)#show route-maps
rfs7000-37FABE(config)#
### 6.1.44 rtls

> show commands

Displays *Real Time Location Service* (RTLS) statistics for access points contributing locationing information.

Supported in the following platforms:
- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
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)#**
6.1.45 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 — AP300, 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, NX7522, NX7532, AP81XX, AP82XX

Syntax

```
show running-config {aaa-policy|association-acl-policy|auto-provisioning-policy|
captive-portal-policy|device|dhcp-server-policy|firewall-policy|include-factory|
interface|ip-access-list|mac-access-list|management-policy|meshpoint|profile|
radio-qos-policy|rf-domain|smart-rf-policy|vlan|wlan|wlan-qos-policy}
```

```
show running-config {aaa-policy|association-acl-policy|auto-provisioning-policy|
captive-portal-policy|dhcp-server-policy|firewall-policy|management-policy|
radio-qos-policy|smart-rf-policy|wlan-qos-policy} <POLICY-NAME> {include-factory}
```

```
show running-config {device [<MAC>|self]} {include-factory}
```

```
show running-config {interface} {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>|mac-access-list <MAC-ACCESS-
LIST-NAME} {include-factory}
```

```
show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}
```

```
show running-config {profile [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|
ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] <PROFILE-NAME}> {include-factory}
```

```
show running-config {rf-domain <DOMAIN-NAME>} {include-factory}
```

```
show running-config {wlan <WLAN-NAME}> {include-factory}
```

Parameters
- show running-config {aaa-policy|association-acl-policy|auto-provisioning-policy|
captive-portal-policy|dhcp-server-policy|firewall-policy|management-policy|
radio-qos-policy|smart-rf-policy|wlan-qos-policy} <POLICY-NAME> {include-factory}

<table>
<thead>
<tr>
<th>running-config</th>
<th>Optional. Displays current running configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-policy</td>
<td>Optional. Displays AAA policy configuration</td>
</tr>
<tr>
<td>association-acl-policy</td>
<td>Optional. Displays association ACL policy configuration</td>
</tr>
<tr>
<td>auto-provisioning-policy</td>
<td>Optional. Displays auto provisioning policy configuration</td>
</tr>
<tr>
<td>captive-portal-policy</td>
<td>Optional. Displays captive portal policy configuration</td>
</tr>
<tr>
<td>dhcp-server-policy</td>
<td>Optional. Displays the DHCP server policy configuration</td>
</tr>
<tr>
<td>firewall-policy</td>
<td>Optional. Displays firewall policy configuration</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show running-config {device [MAC</td>
<td>self]} {include-factory}</td>
</tr>
<tr>
<td>running-config</td>
<td>Displays current running configuration</td>
</tr>
<tr>
<td>device [MAC</td>
<td>self]</td>
</tr>
<tr>
<td>include-factory</td>
<td>Displays device configuration</td>
</tr>
<tr>
<td>running-config</td>
<td>Optional. Displays interface configuration</td>
</tr>
<tr>
<td>interface</td>
<td>Optional. Displays a specified interface configuration. Specify the interface name.</td>
</tr>
<tr>
<td>ge &lt;1-4&gt;</td>
<td>Displays GigabitEthernet interface configuration</td>
</tr>
<tr>
<td>Note: The GE interface range for NX45XX and NX65XX service platforms is &lt;1 - 24&gt;.</td>
<td></td>
</tr>
<tr>
<td>me1</td>
<td>Displays FastEthernet interface configuration</td>
</tr>
<tr>
<td>port-channel &lt;1-2&gt;</td>
<td>Displays port channel interface configuration</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Displays PPP over Ethernet interface configuration</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Displays VLAN interface configuration</td>
</tr>
</tbody>
</table>

management-policy  Optional. Displays management policy configuration
radio-qos-policy    Optional. Displays radio QoS policy configuration
smart-rf-policy     Optional. Displays Smart RF policy configuration
wlan-qos-policy     Optional. Displays WLAN QoS policy configuration

<POLICY-NAME>       The following keyword is common to all policies:
• <POLICY-NAME> – Specify the name of the policy.
include-factory     The following keyword is common to all policies:
• include-factory – Optional. Includes factory defaults

include-factory     Optional. Displays factory defaults

include-factory     Optional. Displays factory defaults
<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</td>
</tr>
<tr>
<td><code>ip-access-list &lt;IP-ACCESS-LIST-NAME&gt;</code></td>
<td>Optional. Displays IP access list configuration</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;IP-ACCESS-LIST-NAME&gt;</code> – Specify the IP access list name</td>
</tr>
<tr>
<td><code>mac-access-list &lt;MAC-ACCESS-LIST-NAME&gt;</code></td>
<td>Optional. Displays MAC access list configuration</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;MAC-ACCESS-LIST-NAME&gt;</code> – Specify the MAC access list name</td>
</tr>
<tr>
<td><code>include-factory</code></td>
<td>The following keyword is common to the 'ip-access-list' and 'mac-access-list' parameters:</td>
</tr>
<tr>
<td></td>
<td>- Optional. Includes factory defaults</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 current running configuration</td>
</tr>
<tr>
<td><code>meshpoint &lt;MESHPOINT-NAME&gt;</code></td>
<td>Optional. Displays meshpoint configuration</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;MESHPOINT-NAME&gt;</code> – Specify the meshpoint name</td>
</tr>
<tr>
<td><code>include-factory</code></td>
<td>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 [ap621</td>
<td>ap622</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>Optional. Displays current configuration for a specified profile</td>
</tr>
<tr>
<td><code>ap621 &lt;PROFILE-NAME&gt;</code></td>
<td>Displays AP621 profile configuration</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;PROFILE-NAME&gt;</code> – Displays configuration for a specified AP621 profile. Specify the AP621 profile name.</td>
</tr>
<tr>
<td><code>ap622 &lt;PROFILE-NAME&gt;</code></td>
<td>Displays AP622 profile configuration</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;PROFILE-NAME&gt;</code> – Displays configuration for a specified AP622 profile. Specify the AP622 profile name.</td>
</tr>
<tr>
<td><code>ap650 &lt;PROFILE-NAME&gt;</code></td>
<td>Displays AP650 profile configuration</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;PROFILE-NAME&gt;</code> – Displays configuration for a specified AP650 profile. Specify the AP650 profile name.</td>
</tr>
<tr>
<td><code>ap6511 &lt;PROFILE-NAME&gt;</code></td>
<td>Displays AP6511 profile</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;PROFILE-NAME&gt;</code> – Displays configuration for a specified AP6511 profile. Specify the AP6511 profile name.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ap6521</td>
<td>Displays AP6521 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP6521 profile. Specify the AP6521 profile name.</td>
</tr>
<tr>
<td>ap6522</td>
<td>Displays AP6522 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP6522 profile. Specify the AP6522 profile name.</td>
</tr>
<tr>
<td>ap6532</td>
<td>Displays AP6532 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP6532 profile. Specify the AP6532 profile name.</td>
</tr>
<tr>
<td>ap6562</td>
<td>Displays AP6562 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP6562 profile. Specify the AP6562 profile name.</td>
</tr>
<tr>
<td>ap71xx</td>
<td>Displays AP71XX profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP71XX profile. Specify the AP71XX profile name.</td>
</tr>
<tr>
<td>ap7502</td>
<td>Displays AP7502 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP7502 profile. Specify the AP7502 profile name.</td>
</tr>
<tr>
<td>ap7522</td>
<td>Displays AP7522 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP7522 profile. Specify the AP7522 profile name.</td>
</tr>
<tr>
<td>ap7532</td>
<td>Displays AP7532 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP7532 profile. Specify the AP7532 profile name.</td>
</tr>
<tr>
<td>ap81xx</td>
<td>Displays AP81XX profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP81XX profile. Specify the AP81XX profile name.</td>
</tr>
<tr>
<td>ap82xx</td>
<td>Displays AP82XX profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified AP82XX profile. Specify the AP82XX profile name.</td>
</tr>
<tr>
<td>rfs4000</td>
<td>Displays RFS4000 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified RFS4000 profile. Specify the RFS4000 profile name.</td>
</tr>
<tr>
<td>rfs6000</td>
<td>Displays RFS6000 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified RFS6000 profile. Specify the RFS6000 profile name.</td>
</tr>
<tr>
<td>rfs7000</td>
<td>Displays RFS7000 profile configuration</td>
</tr>
<tr>
<td>&lt;PROFILE-NAME&gt;</td>
<td>Displays configuration for a specified RFS7000 profile. Specify the RFS7000 profile name.</td>
</tr>
<tr>
<td>nx45xx</td>
<td>Displays NX45XX series service platform profile configuration</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>nx65xx</td>
<td>Displays NX65XX series service platform profile configuration</td>
</tr>
<tr>
<td>nx75xx</td>
<td>Displays NX75XX series service platform profile configuration</td>
</tr>
<tr>
<td>nx9000</td>
<td>Displays NX9000 Series service platform profile configuration</td>
</tr>
<tr>
<td>include-factory</td>
<td>Optional. This parameter is common to all profiles. It includes factory defaults</td>
</tr>
</tbody>
</table>

| running-config | Displays current running configuration | |
| rf-domain <DOMAIN-NAME> | Optional. Displays current configuration for a RF Domain | <DOMAIN-NAME> – Displays current configuration for a specified RF Domain. Specify the RF Domain name. |
| include-factory | Optional. Includes factory defaults | |

| running-config | Displays current running configuration | |
| wlan <WLAN-NAME> | Optional. Displays current configuration for a WLAN | <WLAN-NAME> – Displays current configuration for a specified WLAN. Specify the WLAN name. |
| include-factory | Optional. Includes factory defaults | |

**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  
bride 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)

rfs7000-37FABE(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--
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)#
6.1.46 session-changes

show commands

Displays configuration changes made in the current session

Supported in the following platforms:

- Access Points — AP300, 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, 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)#
### 6.1.47 session-config

- **show commands**

Lists active open sessions on a device.

Supported in the following platforms:

- **Access Points** — AP300, 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, NX81XX, NX82XX

**Syntax**

```
show session-config {include-factory}
```

**Parameters**

- `show session-config {include-factory}`

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session-config</code></td>
<td>Displays current session configuration</td>
</tr>
<tr>
<td><code>include-factory</code></td>
<td>Optional. Includes factory defaults</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config)#show session-config
!
! Configuration of RFS4000 version 5.5.6.0-006D
!
! 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
!
alias network testNetworkAlias address-range 192.168.13.4 to 192.168.13.10
!
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 dhcp 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 1
--More--
rfs4000-229D58(config)#
```
6.1.48 sessions

Displays CLI sessions initiated on a device

Supported in the following platforms:

- Access Points — AP300, 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, 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>
</table>
| on <DEVICE-NAME> | Optional. Displays CLI sessions on a specified device  
|               | • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.                   |

Examples

```
rfs4000-229D58(config)#show sessions
INDEX COOKIE NAME START TIME FROM ROLE
1  49  admin  2014-02-15 15:45:10 192.168.100.225 superuser
2  2   snmp   2014-01-16 22:37:59 127.0.0.1  superuser
3  3   snmp2  2014-01-16 22:37:59 127.0.0.1  superuser
```

rfs4000-229D58(config)#
6.1.49 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:
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
show site-config-diff <SITE-NAME>
```

Parameters
- 

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#
```
**6.1.50 smart-rf**

*show commands*

Displays Smart RF management commands

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show smart-rf [ap|calibration-config|calibration-status|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 [calibration-config|calibration-status|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}
show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on|threshold <50-100>}

**Parameters**

- show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>Displays access point related commands</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. 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>Displays AP related commands</td>
</tr>
<tr>
<td>activity</td>
<td>Optional. Displays AP activity for a specified AP or all APs</td>
</tr>
<tr>
<td>energy</td>
<td>Optional. Displays AP energy for a specified AP or all APs</td>
</tr>
<tr>
<td>neighbors</td>
<td>Optional. Displays AP neighbors</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>The following keywords are common to all of the above parameters:</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>- &lt;MAC&gt; – Displays a specified AP related information. Uses MAC address to identify the AP</td>
</tr>
<tr>
<td>on &lt;DOMAIN-NAME&gt;</td>
<td>- &lt;DEVICE-NAME&gt; – Displays a specified AP related information. Uses device name to identify the AP</td>
</tr>
<tr>
<td>threshold &lt;50-100&gt;</td>
<td>Optional. Displays access point details on a specified RF Domain. Specify the domain name.</td>
</tr>
</tbody>
</table>
- `show smart-rf [calibration-config|calibration-status|channel-distribution|history|history-timeline] {on <DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>calibration-config</td>
<td>Displays interactive calibration configurations</td>
</tr>
<tr>
<td>calibration-status</td>
<td>Displays Smart RF calibration status</td>
</tr>
<tr>
<td>channel-distribution</td>
<td>Displays Smart RF channel distribution</td>
</tr>
<tr>
<td>history</td>
<td>Displays Smart RF calibration history</td>
</tr>
<tr>
<td>history-timeline</td>
<td>Displays extended Smart RF calibration history on an hourly or daily timeline</td>
</tr>
</tbody>
</table>

- `on <DOMAIN-NAME>`

  This parameter is common to all of above Smart RF options:
  - `on <DOMAIN-NAME>` – Optional. Displays Smart RF configuration, based on the parameters passed, on a specified RF Domain
  - `on <DOMAIN-NAME>` – Specify the RF Domain name.

- `show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio</td>
<td>Displays radio related commands</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Optional. Displays details of a specified radio. Specify the radio’s MAC address in the AA-BB-CC-DD-EE-FF format.</td>
</tr>
<tr>
<td>all-11an</td>
<td>Optional. Displays all 11a radios currently in the configuration</td>
</tr>
<tr>
<td>all-11bgn</td>
<td>Optional. Displays all 11bg radios currently in the configuration</td>
</tr>
<tr>
<td>energy &lt;MAC&gt;</td>
<td>Optional. Displays radio energy Specify the MAC address of the radio. Specify the MAC address of the radio in the AA-BB-CC-DD-EE-FF format.</td>
</tr>
</tbody>
</table>

- `on <DOMAIN-NAME>`

  The following keyword is common to above parameters:
  - `on <DOMAIN-NAME>` – Optional. Displays radio details on a specified RF Domain
  - `on <DOMAIN-NAME>` – Specify the RF Domain name.

- `show smart-rf radio {activity|neighbors} {<MAC>|all-11an|all-11bgn} {on <DOMAIN-NAME>}`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio</td>
<td>Displays radio related commands</td>
</tr>
<tr>
<td>activity</td>
<td>Optional. Displays changes related to radio power, number of radio channels, or coverage holes. Use additional filters to view specific details.</td>
</tr>
<tr>
<td>&lt;MAC&gt;</td>
<td>Optional. Displays radio activity for a specified radio Specify the MAC address of the radio. Specify the MAC address of the radio.</td>
</tr>
<tr>
<td>all-11an</td>
<td>Optional. Displays radio activity of all 11a radios in the configuration</td>
</tr>
<tr>
<td>all-11bgn</td>
<td>Optional. Displays radio activity of all 11bg radios in the configuration</td>
</tr>
</tbody>
</table>

- `on <DOMAIN-NAME>`

  Optional. Displays radio activity of all radios within a specified RF Domain
  - `on <DOMAIN-NAME>` – Specify the RF Domain name.
• **show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>|on}**

<table>
<thead>
<tr>
<th>interfering-ap</th>
<th>Displays interfering access points (requiring potential isolation) information</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;</td>
<td>Optional. Displays information of a specified interfering access point</td>
</tr>
<tr>
<td></td>
<td>• &lt;MAC&gt; – Specify the access point’s MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Considers all APs if this parameter is omitted</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays interfering access point information on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the device name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Considers all APs if this parameter is omitted</td>
</tr>
<tr>
<td>on &lt;DOMAIN-NAME&gt;</td>
<td>Optional. Displays all interfering access point information within a specified RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</td>
</tr>
</tbody>
</table>

• **show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>|on|threshold <50-100>}**

<table>
<thead>
<tr>
<th>interfering-ap</th>
<th>Displays interfering neighboring access point information</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;</td>
<td>Optional. Displays interfering neighboring access point information</td>
</tr>
<tr>
<td></td>
<td>• &lt;MAC&gt; – Specify the access point’s MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Considers all APs if this parameter is omitted</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays all interfering neighboring access point information on a specified device</td>
</tr>
<tr>
<td></td>
<td>• &lt;DEVICE-NAME&gt; – Specify the device name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Considers all APs if this parameter is omitted</td>
</tr>
<tr>
<td>threshold &lt;50-100&gt;</td>
<td>Specifies the maximum attenuation threshold of interfering neighbors. Specify a value from 50 - 100.</td>
</tr>
<tr>
<td>on &lt;DOMAIN-NAME&gt;</td>
<td>Optional. Displays radio activity of all radios within a specified RF Domain</td>
</tr>
<tr>
<td></td>
<td>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</td>
</tr>
</tbody>
</table>

**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)#
### 6.1.51 spanning-tree

**show commands**

Displays spanning tree utilization information.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

- `show spanning-tree mst {configuration|detail|instance|on}
- 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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree</td>
<td>Displays spanning tree utilization information</td>
</tr>
<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></td>
</tr>
<tr>
<td>detail</td>
<td>Optional. Displays detailed MST configuration, based on the parameters passed</td>
</tr>
</tbody>
</table>

**Show spanmng-tree mst {configuration} {on <DEVICE-NAME>}:**
- **configuration**
- **instance**
- **interface**

**Parameters:**
- `show spanning-tree mst {configuration} {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree</td>
<td>Displays spanning tree utilization information</td>
</tr>
<tr>
<td>mst</td>
<td>Displays MST configuration</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed MST configuration for a specified interface</td>
</tr>
</tbody>
</table>

Note: The GE interface range for NX45XX and NX65XX service platforms is <1 - 24>
### show spanning-tree mst

- **instance <1-15>** - Specify the instance ID from 1 - 15.
- **interface <INTERFACE-NAME>** - Displays MST configuration for a specified interface instance. Specify the interface name.
- **on <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 portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
```

```
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

% ge4: Port 2004 - Id 87d4 - Role Disabled - State Forwarding
% ge4: Designated External Path Cost 0 - Internal Path Cost 0
% ge4: Configured Path Cost 11520 - Add type Implicit - ref count 1
% ge4: Designated Port Id 0 - CST Priority 128
% ge4: ge4: CIST Root 0000000000000000
% ge4: ge4: Regional Root 0000000000000000
% ge4: ge4: Designated Bridge 0000000000000000
% ge4: Message Age 0 - Max Age 0
% ge4: CIST Hello Time 0 - Forward Delay 0
% ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
% --More--

rfs7000-37FABE(config)#
rfs7000-37FABE(config)#show spanning-tree mst instance 1 interface test
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
% 1: portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
% --More--

rfs7000-37FABE(config)#
6.1.52 startup-config

Displays complete startup configuration script

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
show startup-config

{include-factory}
```

Parameters

- `show startup-config {include-factory}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Displays startup configuration script</td>
</tr>
<tr>
<td>include-factory</td>
<td>Optional. Includes factory defaults</td>
</tr>
</tbody>
</table>

Examples

```
rfs4000-229D58(config)#show startup-config

! Configuration of RFS4000 version 5.5.6.0-006D
!
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)#
```
6.1.53 terminal

show commands

Displays terminal configuration parameters

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

show terminal

Parameters

None

Examples

rfs7000-37FABE(config)#show terminal
Terminal Type: xterm
Length: 24 Width: 200
rfs7000-37FABE(config)#
6.1.54 timezone

- show commands

Displays a device's timezone

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

show timezone

Parameters

None

Examples

rfs7000-37FABE(config)#show timezone
Timezone is America/Los_Angeles
rfs7000-37FABE(config)#
6.1.55 upgrade-status

- show commands

Displays the last image upgrade status

**NOTE:** This command is not available in the USER EXEC Mode.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show upgrade-status {detail|on}
show upgrade-status {detail} {on <DEVICE-NAME>}
```

**Parameters**
- `show upgrade-status {detail} {on <DEVICE-NAME>}`
  - `upgrade-status` Displays last image upgrade status and log
  - `detail` Optional. Displays last image upgrade status in detail
  - `on <DEVICE-NAME>` 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.

**Examples**

```
rfs4000-229D58(config)# show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2014-04-10 09:10:05

rfs4000-229D58(config)#
```

```
rfs4000-229D58(config)# show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2013-11-11 14:05:55

Running from partition /dev/mtdblock7
var2 is 3 percent full
/tmp is 5 percent full
Free Memory 114464 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 5.5.6.0-006D
Writing Kernel to /dev/mtd4
Writing BootOS to /dev/mtd2
Successful

rfs4000-229D58(config)#
```
6.1.56 version

> show commands

Displays a device’s software and hardware version

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
show version {on <DEVICE-NAME>}

Parameters
- show version {on <DEVICE-NAME>}

<table>
<thead>
<tr>
<th>version {on &lt;DEVICE-NAME&gt;}</th>
<th>Displays software and hardware versions on all devices or a specified device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• on &lt;DEVICE-NAME&gt; – Optional. Displays software and hardware versions 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(config)#show version
RFS4000 version 5.5.6.0-006D
Copyright (c) 2004-2014 Company All rights reserved.
Booted from primary

rfs4000-229D58 uptime is 14 days, 03 hours 55 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 2.28
Radio HAL version is 92 (DFS:73)

rfs4000-229D58(config)#
6.1.57 vrrp

Displays **Virtual Router Redundancy Protocol (VRRP)** protocol details

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show vrrp [brief|details|stats] {<1-255>} {on <DEVICE-NAME>}
show vrrp error-stats {on <DEVICE-NAME>}
```

**Parameters**

- `show vrrp [brief|details|stats] {<1-255>} {on <DEVICE-NAME>}`
  - brief Displays virtual router information in brief
  - details Displays virtual router information in detail
  - stats Displays virtual router statistics
  - `<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>}`
  - 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**

```
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)#
```
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)#
### 6.1.58 what

> **show commands**

Displays details of a specified search phrase (performs global search)

Supported in the following platforms:

- **Access Points** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}
```

**Parameters**

- **show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>**

<table>
<thead>
<tr>
<th>contain &lt;WORD&gt;</th>
<th>Searches on all the items that contain a specified word</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;WORD&gt; – Specify a word to search (for example, MAC address, hostname etc.).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>is &lt;WORD&gt;</th>
<th>Searches on an exact match</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt;</td>
<td>&lt;WORD&gt; – Specify a word to search (for example, MAC address, hostname etc.).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</th>
<th>Optional. Performs global search on a specified device or RF Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DEVICE-OR-DOMAIN-NAME&gt;</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>

**Examples**

```
rfs4000-229D58#show what contain default
---------------------------------------------------------------------------------------
NO.  CATEGORY             MATCHED                        OTHER KEY INFO (1)             OTHER                   OTHER  
KEY INFO (2)             OTHER KEY INFO (3) NAME/VALUE             NAME/VALUE NAME/VALUE NAME/VALUE NAME/VALUE NAME/VALUE NAME/VALUE
---------------------------------------------------------------------------------------
https-trustpoint               type                       mac                            rf_domain_name
1   device-cfg       default-trustpoint rfs4000      00-23-68-22-9D-58              default
__obj_name__                   name
2   firewall_policy      default                        default                        True
__obj_name__                   name                           https
idle_session_timeout
3   management_policy    default                        default                        True
30    qos_policy                     name                           control_vlan
```

```bash
--More--
rfs4000-229D58#
```
6.1.59 wireless

Displays wireless configuration parameters

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510

Syntax

show wireless [ap|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 client {association-history|detail|filter|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]}
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 {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 <DEVICE-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 {detail} {filter <RADIO-MAC>} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio {statistics} {detail|on|rf|windows-data}
show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>}
{rf {on <DEVICE-OR-DOMAIN-NAME>}}
show wireless radio {statistics} {detail|window-data} {<DEVICE-NAME>}{<1-3>}
{filter <RADIO-MAC>} {on <DEVICE-OR-DOMAIN-NAME>}}
show wireless radio {tspec} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>|option}
show wireless radio {wlan-map} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless regulatory [channel-info <WORD>|country-code <WORD>|device-type]
show wireless regulatory device-type [ap300|ap621|ap622|ap650|ap6511|ap6521|ap6522|
ap6532|ap6562|ap7131|ap7161|ap7181|ap71xx|ap7502|ap7522|ap7532|ap82xx|rfs4000|rfs6000|
rfs7000] <WORD>

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 {detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|
usage-mappings}
show wireless {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

<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>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
</tr>
<tr>
<td>ap</td>
<td>Displays managed access point information</td>
</tr>
<tr>
<td>detail</td>
<td>Optional. Displays detailed information for all APs or a specified AP</td>
</tr>
<tr>
<td>&lt;MAC/HOST-NAME&gt;</td>
<td>- Optional. Displays information for 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></td>
<td>- on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays 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>

- show wireless ap

<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>load-balancing {client-capability</td>
<td>events</td>
</tr>
<tr>
<td>client-capability</td>
<td>- Optional. Displays client band capability</td>
</tr>
<tr>
<td>events</td>
<td>- Optional. Displays client events</td>
</tr>
<tr>
<td>neighbors</td>
<td>- Optional. Displays neighboring clients</td>
</tr>
</tbody>
</table>

- show wireless ap

<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>load-balancing {client-capability</td>
<td>events</td>
</tr>
<tr>
<td>client-capability</td>
<td>- Optional. Displays client band capability</td>
</tr>
<tr>
<td>events</td>
<td>- Optional. Displays client events</td>
</tr>
<tr>
<td>neighbors</td>
<td>- Optional. Displays neighboring clients</td>
</tr>
</tbody>
</table>
| 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. |

- **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 |
| detail <MAC> | Optional. Displays detailed wireless client(s) information
  - <MAC> – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client. |
| 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** {filter ip [<IP>|not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}

| wireless | Displays wireless configuration parameters |
| client | Displays client information based on the parameters passed |
| filter IP [<IP>|not <IP>] | Optional. Uses IP addresses to filter wireless clients
  - <IP> – Selects clients with IP address matching the <IP> parameter
  - not <IP> – Inverts the match selection |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'IP' and 'not IP' parameters:
  - on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected wireless client 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 {filter} {state [data-ready|not [data-ready|roaming]]|roaming} {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>filter state</td>
<td>Optional. Filters clients based on their state</td>
</tr>
<tr>
<td>data-ready</td>
<td>Selects wireless clients in the data-ready state</td>
</tr>
<tr>
<td>not [data-ready]</td>
<td>Inverts match selection. Selects wireless clients neither ready nor roaming</td>
</tr>
<tr>
<td>roaming</td>
<td>Selects roaming clients</td>
</tr>
</tbody>
</table>

- `on <DEVICE-OR-DOMAIN-NAME>`

| The following keyword is common to the ‘ready’, ‘not’, and ‘roaming’ parameters: |
| on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected client details on a specified device or RF Domain |

- `show wireless client {filter} {wlan [<WLAN-NAME]|not <WLAN-NAME>} {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>filter wlan</td>
<td>Optional. Filters clients on a specified WLAN</td>
</tr>
<tr>
<td>&lt;WLAN-NAME&gt;</td>
<td>Specify the WLAN name.</td>
</tr>
<tr>
<td>not &lt;WLAN-NAME&gt;</td>
<td>Inverts the match selection</td>
</tr>
</tbody>
</table>

- `on <DEVICE-OR-DOMAIN-NAME>`

| 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 |

- `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>
<tr>
<td>statistics</td>
<td>Optional. Displays detailed client statistics. Use additional filters to view specific details.</td>
</tr>
<tr>
<td>detail &lt;MAC&gt;</td>
<td>Optional. Displays detailed client statistics</td>
</tr>
<tr>
<td>rf</td>
<td>Optional. Displays detailed client statistics on a specified device or RF Domain</td>
</tr>
<tr>
<td>window-data &lt;MAC&gt;</td>
<td>Optional. Displays historical data, for a specified client</td>
</tr>
</tbody>
</table>

- `on <DEVICE-OR-DOMAIN-NAME>`

| 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 |
### SHOW COMMANDS 6 - 115

#### show wireless client {tspec} {<MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

- **wireless**: Displays wireless configuration parameters
- **client**: Displays client information based on the parameters passed
- **tspec <MAC>**: Optional. Displays detailed traffic specification (TSPEC) information for all clients or a specified client
  - `<MAC>` – Optional. Displays detailed TSPEC information for a specified client. Specify the MAC address of the client.
- **on <DEVICE-OR-DOMAIN-NAME>**: The following keyword is recursive and common to the ‘tspec <MAC>’ parameter:
  - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain.

#### show wireless meshpoint {config} {filter [device <DEVICE-NAME> | rf-domain <DOMAIN-NAME>]}<MESHPOINT-NAME>

- **wireless**: Displays wireless configuration parameters
- **meshpoint**: Displays meshpoint related information
- **config**: Optional. Displays all meshpoint configuration
- **filters**: Optional. Provides additional filter options, such as device name and RF Domain name.
  - `<DEVICE-NAME>` – Displays meshpoints applied to a specified device
  - `<DOMAIN-NAME>` – Specify the domain name

#### show wireless meshpoint {detail} {<MESHPOINT-NAME>}

- **wireless**: Displays wireless configuration parameters
- **meshpoint**: Displays meshpoint related information
- **detail**: 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>] {on <DEVICE-OR-DOMAIN-NAME>}

- **wireless**: Displays wireless configuration parameters
- **meshpoint**: Displays meshpoint related information
- **multicast**: Optional. Displays meshpoint multicast information
- **path**: Optional. Displays meshpoint path information
- **proxy**: Optional. Displays meshpoint proxy information
- **root**: Optional. Displays meshpoint root information
### show wireless meshpoint

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>Optional. Displays meshpoint security information</td>
</tr>
<tr>
<td>statistics</td>
<td>Optional. Displays meshpoint statistics</td>
</tr>
<tr>
<td><code>&lt;MESHPOINT-NAME&gt;</code></td>
<td>The following keywords are common to all of the above parameters:</td>
</tr>
<tr>
<td>detail</td>
<td>• <code>&lt;MESHPOINT-NAME&gt;</code> – Displays meshpoint related information for a specified meshpoint. Specify the meshpoint name.</td>
</tr>
<tr>
<td></td>
<td>• <code>detail</code> – Displays detailed multicast information for all meshpoints</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>The following keyword is common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• on <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code> – Optional. Displays detailed multicast information on a specified device or RF Domain.</td>
</tr>
</tbody>
</table>

#### Command Example

```
show wireless meshpoint {neighbor} [<MESHPOINT-NAME>|detail|statistics {rf}] {on <DEVICE-OR-DOMAIN-NAME>}
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless</td>
<td>Displays wireless configuration parameters</td>
</tr>
<tr>
<td>neighbor</td>
<td>Optional. Displays meshpoint neighbor information, based on the parameters passed</td>
</tr>
<tr>
<td><code>&lt;MESHPOINT-NAME&gt;</code></td>
<td>Select one of the following parameter to view neighbor related information</td>
</tr>
<tr>
<td>detail</td>
<td>statistics <code>{rf}</code></td>
</tr>
<tr>
<td></td>
<td>• <code>detail</code> – Displays detailed multicast information for all meshpoints</td>
</tr>
<tr>
<td></td>
<td>• <code>statistics</code> – Displays neighbors related statistics</td>
</tr>
<tr>
<td></td>
<td>• <code>{rf}</code> – Optional. Displays RF related statistics for neighbors</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>The following keyword is common to all of the above parameters:</td>
</tr>
<tr>
<td></td>
<td>• on <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code> – Optional. Displays meshpoint neighbor information, based on the parameters passed, on a specified device or RF Domain.</td>
</tr>
</tbody>
</table>

#### Command Example

```
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint</td>
<td>Displays meshpoint related information</td>
</tr>
<tr>
<td><code>tree</code></td>
<td>Optional. Displays meshpoint network tree</td>
</tr>
<tr>
<td>on <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code></td>
<td>Optional. Displays meshpoint network tree on a specified device or RF Domain</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEVICE-OR-DOMAIN-NAME&gt;</code> – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain</td>
</tr>
</tbody>
</table>

#### Command Example

```
show wireless meshpoint {usage-mappings} {on <DEVICE-OR-DOMAIN-NAME>}
```

<table>
<thead>
<tr>
<th>Keyword</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>SHOW COMMANDS 6 - 117</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>show wireless mobility-database {on &lt;DEVICE-NAME&gt;]</strong></td>
<td></td>
</tr>
</tbody>
</table>

- `wireless` Displays wireless configuration parameters
- `mobility-database` Displays controller-assisted mobility database
- `on <DEVICE-OR-DOMAIN-NAME>`
  - Optional. Displays meshpoint applied to a specified device or RF Domain
  - `<DEVICE-OR-DOMAIN-NAME>` – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain

**Example:**

- `show wireless mobility-database {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>SHOW COMMANDS 6 - 117</th>
</tr>
</thead>
<tbody>
<tr>
<td>**show wireless radio {detail} {&lt;DEVICE-NAME&gt; {&lt;1-3&gt;</td>
</tr>
</tbody>
</table>

- `wireless` Displays wireless configuration parameters
- `radio` Displays radio operation status and other related information
- `detail` Optional. Displays detailed radio operation status
- `<DEVICE-NAME>` 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.
- `<1-3>` Optional. Specify the radio interface index from 1 - 3 (if not specified as part of the radio ID)
- `filter <RADIO-MAC>` Optional. Provides additional filter options
  - `<RADIO-MAC>` – Optional. Filters based on the radio MAC address
  - `<DEVICE-OR-DOMAIN-NAME>` – 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.

**Example:**

- `show wireless radio {detail} {filter <RADIO-MAC>} {on <DEVICE-OR-DOMAIN-NAME>}`
- **show wireless radio** {statistics} {on <DEVICE-OR-DOMAIN-NAME>}
  rf {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>radio</td>
<td>Displays radio operation status and other related information</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</td>
</tr>
</tbody>
</table>
  - <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
| rf {on <DEVICE-OR-DOMAIN-NAME>} | Optional. Displays RF statistics 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 radio** {statistics} {detail|window-data} {<DEVICE-NAME>} {<1-3>} filter <RADIO-MAC> {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>radio</td>
<td>Displays radio operation status and other related information</td>
</tr>
<tr>
<td>statistics</td>
<td>Optional. Displays radio traffic and RF statistics</td>
</tr>
</tbody>
</table>
  - detail – Displays detailed traffic and RF statistics of all radios
  - window-data – Displays historical data over a time window
| <DEVICE-NAME> <1-3>     | The following keywords are common to the ‘detail’ and ‘window-data’ parameters:
  - <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.
  - <1-3> – Optional. Specify the radio interface index. |
| filter <RADIO-MAC>      | Optional. Provides additional filters                                        |
  - <RADIO-MAC> – Optional. Filters based on the radio MAC address             |
| on <DEVICE-OR-DOMAIN-NAME> | 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 wireless radio** {tspec} {<DEVICE-NAME> | filter| on <DEVICE-OR-DOMAIN-NAME> | option}

<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</td>
</tr>
<tr>
<td>tspec</td>
<td>Optional. Displays TSPEC information on a radio</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
### SHOW COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless regulatory channel-info &lt;WORD&gt;</td>
<td>Displays channel information. Optional. &lt;WORD&gt; – Specify the channel number.</td>
</tr>
<tr>
<td>show wireless regulatory country-code &lt;WORD&gt;</td>
<td>Displays country code to country name information. Optional. &lt;WORD&gt; – Specify the two letter ISO-3166 country code.</td>
</tr>
<tr>
<td>show wireless regulatory device-type [ap300</td>
<td>ap621</td>
</tr>
</tbody>
</table>
### show wireless rf-domain statistics

<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

<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>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</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

<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>statistics</td>
<td>Optional. Displays channel statistics</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is common to the ‘detailed’ and ‘statistics’ parameters:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain</td>
</tr>
</tbody>
</table>

### show wireless wips

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>wips [client-blacklist</td>
<td>event-history] {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</td>
</tr>
<tr>
<td>client-blacklist</td>
<td>Displays blacklisted clients</td>
</tr>
<tr>
<td>event-history</td>
<td>Displays event history</td>
</tr>
<tr>
<td>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</td>
<td>The following keyword is common to the ‘client-blacklist’ and ‘event-history’ parameters:</td>
</tr>
<tr>
<td></td>
<td>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain</td>
</tr>
</tbody>
</table>
- **show wlan** `{detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|policy-mappings|usage-mappings}`

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>Displays WLAN related information based on the parameters passed</td>
</tr>
</tbody>
</table>
| detail <WLAN>     | Optional. Displays WLAN configuration  
|                   |   - `<WLAN>` – Specify the WLAN name. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays WLAN configuration on a specified device or RF Domain  
|                   |   - `<DEVICE-OR-DOMAIN-NAME>` – Specify the name of the AP, wireless controller, service platform, or RF Domain. |
| policy-mappings   | Optional. Displays WLAN policy mappings |
| usage-mappings    | Optional. Lists all devices and profiles using the WLAN |

- **show wlan** `{config filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}}`

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>Displays WLAN related information based on the parameters passed</td>
</tr>
<tr>
<td>config filter</td>
<td>Optional. Filters WLAN information based on the device name or RF Domain</td>
</tr>
</tbody>
</table>
| device <DEVICE-NAME> | Optional. Filters WLAN information based on the device name  
|                   |   - `<DEVICE-NAME>` – Specify the device name. |
| rf-domain <DOMAIN-NAME> | Optional. Filters WLAN information based on the RF Domain  
|                   |   - `<DOMAIN-NAME>` – Specify the RF Domain name. |

- **show wlan** `{statistics {<WLAN>|detail} {(on <DEVICE-OR-DOMAIN-NAME>))}}`

<table>
<thead>
<tr>
<th>wireless</th>
<th>Displays wireless configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>Displays WLAN related information based on the parameters passed</td>
</tr>
</tbody>
</table>
| statistics        | Optional. Displays WLAN statistics. Use additional filters to view specific details  
|                   |   - `<WLAN>` – Optional. Displays WLAN statistics. Specify the WLAN name.  
|                   |   - `detail` – Optional. Displays detailed WLAN statistics |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the ‘WLAN’ and ‘detail’ parameters:  
|                   |   - on `<DEVICE-OR-DOMAIN-NAME>` – Optional. Displays WLAN statistics on a specified device or RF Domain |
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-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-meshpoint                   Customize the output of (show wireless meshpoint) 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
---------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VENDOR</th>
<th>RADIO-ID</th>
<th>WLAN</th>
<th>VLAN</th>
<th>STATE</th>
</tr>
</thead>
</table>
---------------------------------------------------------------------------------------
```

Total number of wireless clients displayed: 0

```
rfs7000-37FABE(config)#
```

The above output can be customized, using the `customize > show-wireless-client` command, as follows:

```
rfs7000-37FABE(config)#customize show-wireless-client mac ip vendor vlan radio-id state wlan location radio-alias radio-type
rfs7000-37FABE(config)#commit
```

```
rfs7000-37FABE(config)#show wireless client
---------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VENDOR</th>
<th>RADIO-ID</th>
<th>WLAN</th>
<th>STATE</th>
</tr>
</thead>
</table>
---------------------------------------------------------------------------------------
```

Total number of wireless clients displayed: 0

```
rfs7000-37FABE(config)#
```

For more information on the customize command, see `customize on page 4-88`. 
Examples

rfs7000-37FABE(config)#show wireless wips mu-blacklist
No mobile units blacklisted

rfs7000-37FABE(config)#show wireless wlan config
+-----------+---------+-----------+-------------+-----------------+-------
|    NAME   |  ENABLE |    SSID   |  ENCRYPTION |  AUTHENTICATION |    VLAN |
+-----------+---------+-----------+-------------+-----------------+-------
| test      | Y       | test      | none        | none            | 1     |
| company   | Y       | company   | none        | none            | 1     |
| wlan1     | Y       | wlan1     | none        | none            | 1     |

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless wlan statistics
+---------------------+----------+----------+--------+--------+--------+--
|         WLAN        | TX BYTES | RX BYTES |TX PKTS |RX PKTS |TX KBPS |RX KBPS |
| ERRORS |
+---------------------+----------+----------+--------+--------+--------+--
|            company |        0 |        0 |      0 |      0 |      0 |      0 |      0 |      0  |
|               wlan1 |        0 |        0 |      0 |      0 |      0 |      0 |      0 |      0  |
+---------------------+----------+----------+--------+--------+--------+--
Total number of wlan displayed: 2

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory channel-info 1
Center frequency for channel 1 is 2412MHz

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory country-code
ISO CODE   NAME
---
    al    Algeria
    ai    Anguilla
    ar    Argentina
    au    Australia
    at    Austria
    bs    Bahamas
    bh    Bahrain
    bb    Barbados
    by    Belarus
    be    Belgium
    bm    Bermuda

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory device-type ap650 in
+----------+----------+-----------+--------+--------+--------+--
|   #      | Channel Set | Power (mW) | Power (dBm) | Placement | DFS       | CAC(mins) | TPC     |
+----------+----------+-----------+--------+-----------+----------+----------+--------
|          1 | 1-13     | 1000      | 30     | Indoor/Outdoor | NA       | NA       | NA     |
|          2 | 149-165  | 200       | 23     | Indoor      | Not Required | 0        | Not Required |
|          3 | 36-64    | 200       | 23     | Indoor      | Not Required | 0        | Not Required |
|          4 | 149-165  | 1000      | 30     | Outdoor     | Not Required | 0        | Not Required |

rfs7000-37FABE(config)#
rfs7000-6DCD4B(config)#show wireless ap detail

AP: 00-23-68-22-9D-58
AP Name: rfs4000-229D58
Location: default
RF-Domain: default
Type: rfs4000
Model: RFS-4010-00010-WR
IP: 192.168.0.1
Num of radios: 0
Num of clients: 0
Last Smart-RF time: not done
Stats update mode: auto
Stats interval: 31
Radio Modes:
  radio-1: None
Country-code: not-set
Site-Survivable: True
Last error:
Fault Detected: False

AP: B4-C7-99-58-72-58
AP Name: ap5142-587258
Location: default
RF-Domain: default
Type: ap5142
Model: AP-5142-66040-WR
IP: 192.168.13.24
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: not-set
Site-Survivable: True
Last error:
Fault Detected: False

AP: B4-C7-99-71-17-28
AP Name: ap81xx-711728
Location: default
RF-Domain: default
Type: ap81xx
Model: AP-8132-66040-US
IP: 192.168.13.25
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: not-set
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: 3
rfs7000-6DCD4B(config)#
show wireless ap load-balancing on default

AP: 00-23-68-11-E6-C4
Client requests on 5ghz : allowed
Client requests on 2.4ghz : allowed

Average AP load in neighborhood               : 0 %
Load on this AP                               : 0 %
Total 2.4ghz band load in neighborhood        : 0 %
Total 5ghz band load in neighborhood          : 0 %
Configured band ratio 2.4ghz to 5ghz          : 1:1
Current band ratio 2.4ghz to 5ghz             : 0:0
Average 2.4ghz channel load in neighborhood   : 0 %
Average 5ghz channel load in neighborhood     : 0 %
Load on this AP's 2.4ghz channel              : 0 %
Load on this AP's 5ghz channel                : 0 %

Total number of APs displayed: 1

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
LAST-CAL-TIME

rfs4000-229D58 default default 00-23-68-11-E6-C4   2   W-W     0
not done

Total number of APs displayed: 1

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

show wireless meshpoint

MESH              HOSTNAME          HOPS IS-ROOT CONFIG-AS-ROOT ROOT-HOSTNAME       ROOT-BOUND-TIME NEXT-HOP-HOSTNAME NEXT-HOP-USE-TIME

   c00466 ap7131-96F998        1 NO      NO             ap7131-96FAAC       1 days 02:01:33 ap7131-96FAAC
   c00466 ap7131-96FAAC        0 YES     YES            N/A                             N/A
   c00466 ap7131-96F6B4        2 NO      NO             ap7131-96FAAC       1 days 02:01:31 ap7131-96FAAC

Total number of meshpoint displayed: 3
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

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>RMet Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>5C-0E-8B-21-76-22.5C-0E-EB-21-74-40</td>
<td>00-23-68-2E-97-60</td>
<td>115</td>
<td>0</td>
<td>97</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>00-23-68-30-F7-82.00-23-68-30-F8-F0</td>
<td>00-23-68-2E-97-60</td>
<td>99</td>
<td>1</td>
<td>97</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>5C-0E-8B-21-76-22.5C-0E-8B-21-76-22</td>
<td>00-23-68-2E-97-60</td>
<td>115</td>
<td>1</td>
<td>97</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>5C-0E-8B-21-76-22.5C-0E-EB-21-74-40</td>
<td>00-23-68-2E-97-60</td>
<td>115</td>
<td>1</td>
<td>97</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>00-23-68-2E-AB-50.00-23-68-2E-AB-50</td>
<td>00-23-68-2E-97-60</td>
<td>0</td>
<td>0</td>
<td>97</td>
</tr>
<tr>
<td>Root 00-23-68-00-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>7</td>
<td>96</td>
<td>94</td>
</tr>
<tr>
<td>00-23-68-2E-97-60.00-23-68-2E-97-60</td>
<td>00-23-68-2E-97-60</td>
<td>0</td>
<td>0</td>
<td>97</td>
</tr>
<tr>
<td>Root 00-23-68-00-00-00-01:R2 Enabled</td>
<td>Yes</td>
<td>8</td>
<td>94</td>
<td>90</td>
</tr>
</tbody>
</table>

Total number of meshpoint displayed: 1

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>00-23-68-00-00-01</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

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

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>
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</th>
<th>Hops</th>
<th>Type</th>
<th>Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00-23-68-2E-AB-50</td>
<td>00-23-68-2E-AB-50</td>
<td>Valid 1</td>
<td>Root</td>
<td>Bound</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>8730</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</td>
<td>Valid 1</td>
<td>Root</td>
<td>Unbound</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>5200</td>
<td>3481</td>
<td>68.31.1A.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

rfs4000-22A24E#show wireless client

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>
<th>VLAN</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-01-02-03-04-10</td>
<td>2.3.4.16</td>
<td>3Com Corp</td>
<td>00-01-02-03-04-00:R1</td>
<td>sim-wlan-1</td>
<td>1</td>
<td>Data-Ready</td>
</tr>
<tr>
<td>00-01-02-03-05-10</td>
<td>2.3.5.16</td>
<td>3Com Corp</td>
<td>00-01-02-03-04-00:R2</td>
<td>sim-wlan-1</td>
<td>1</td>
<td>Data-Ready</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>
<th>VLAN</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-01-02-03-04-10</td>
<td>2.3.4.16</td>
<td>3Com Corp</td>
<td>00-01-02-03-04-00:R1</td>
<td>sim-wlan-1</td>
<td>1</td>
<td>Data-Ready</td>
</tr>
<tr>
<td>00-01-02-03-05-10</td>
<td>2.3.5.16</td>
<td>3Com Corp</td>
<td>00-01-02-03-04-00:R2</td>
<td>sim-wlan-1</td>
<td>1</td>
<td>Data-Ready</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#
6.1.60 `wwan`

Displays wireless WAN status

Supported in the following platforms:
- Access Points — AP300, 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, 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>wwan</th>
<th>Displays wireless WAN configuration and status details</th>
</tr>
</thead>
<tbody>
<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>
</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)#
```
6.1.61 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**

- show slot

| show slot | Shows PCI express card statistics |

**Examples**

nx4500-5CFA2B>show slot

```
----------------------------
SLOT  TYPE   MODULE   STATUS
----------------------------
 1   []  wing   Enabled
 2   []  wing   Enabled
 3   []  wing   Enabled
 4   []  wing   Enabled
----------------------------
nx4500-5CFA2B>
```
### 6.1.62 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-cache-policy`.

Supported in the following platforms:
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### 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|      0.0|         0|         0
-------------------------------------------------------------------
nx4500-5CFA2B>
nx4500-5CFA2B(config)#show smart-cache statistics content-type
```

```
-----------------------------------------------------------------------
 DURATION   |     VIDEO (KB)     |     AUDIO (KB)     |     IMAGE (KB)     |     TEXT
|   TOTAL      CACHE  |   TOTAL      CACHE  |   TOTAL      CACHE  |   TOTAL
|TOTAL CACHE  |    TOTAL CACHE  |
---------------|-----------------|-----------------|-----------------|------|------|------|
Since boot |         0|         0|         0|         0|         0|         0
-----------------------------------------------------------------------
nx4500-5CFA2B(config)#
```
nx4500-5CFA2B#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#
6.1.63 virtual-machine

> show commands

Displays the virtual-machine (VM) configuration, logs, and statistics

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9500, NX9510, NX9600

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>)}

| configuration | Displays detailed VM configuration |
| statistics    | Displays VM statistics            |
| <[<VM-NAME>|team-urc|team-rls|team-vowlan]> | The following keywords are common to the 'configuration' and 'statistics' parameters: |
|               | • <VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. |
|               | • team-urc – Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics |
|               | • team-rls – Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/statistics |
|               | • team-vowlan – Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics |
| Note:        | These keywords are specific to the NX45XX and NX65XX series service platforms. |
| on <DEVICE-NAME> | Specifies the name of the device on which the command is executed |
|               | • <DEVICE-NAME> – Specify the name of the service platform. |

- show virtual-machine [configuration|statistics] {<VM-NAME>|adsp|team-cmt} {on <DEVICE-NAME>}

| configuration | Displays detailed VM configuration |
| statistics    | Displays VM statistics            |
| [<VM-NAME>|adsp|team-cmt] | The following keywords are common to the 'configuration' and 'statistics' parameters: |
|               | • <VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. |
|               | • adsp – Optional. Displays Air-Defense Services Platform (ADSP) VM configuration/statistics |
|               | • team-cmt – Optional. Displays TEAM-CMT VM configuration/statistics |
| Note:        | These keywords are specific to the NX9500 and NX9510 service platforms. |
### SHOW COMMANDS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show virtual-machine debugging</strong> {level[debug</td>
<td>error</td>
</tr>
<tr>
<td><strong>show virtual-machine export</strong> &lt;VM-NAME&gt; {on &lt;DEVICE-NAME&gt;}}</td>
<td>Displays VM configuration export related information for the virtual machine identified by the <code>&lt;VM-NAME&gt;</code> keyword. Specify the VM name. <strong>Note:</strong> The NX9500 and NX9510 series service platforms will display ADSP and TEAM-CMT VM configuration export information</td>
</tr>
</tbody>
</table>

### 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            : b80f8e19-1af6-02c9-cbbc-10c1aeb0a170
  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#
```
### 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>

### 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>4</td>
<td>1009</td>
<td>-</td>
<td>-</td>
</tr>
<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>

The following example shows WiNG memory allocation on a NX9500 device:

### 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>-</td>
<td>unknown</td>
<td>-</td>
</tr>
</tbody>
</table>

### 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>

### show virtual-machine statistics adsp

VM name: adsp
Base Version : unknown
Install Status : not_installed
6.1.64 mirroring

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

```text
show mirroring
```

Parameters

```text
- show mirroring
```

<table>
<thead>
<tr>
<th>show mirroring</th>
<th>Displays the port mirroring sessions</th>
</tr>
</thead>
</table>

Examples

```text
nx4524-470984# show mirroring

+-------+-------+-------+-------+
| Session| Source | Destination | Direction |
|--------+-------+------------+-----------|
| 1      | ge3   | ge24       | any       |
| 2      | ge7   | ge24       | inbound   |
| 3      | ge5   | ge24       | outbound  |

nx4524-470984#
```
### 6.1.65 `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, NX9600, NX7500

**Syntax**

```
show raid {on <DEVICE-NAME>}
```

**Parameters**

- `show raid {on <DEVICE-NAME>}`

<table>
<thead>
<tr>
<th>show raid</th>
<th>Displays the RAID array status and statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>on &lt;DEVICE-NAME&gt;</td>
<td>Optional. Displays RAID status and statistics on a specified device</td>
</tr>
</tbody>
</table>

- `<DEVICE-NAME>` – Specify the name of the AP, wireless controller, or service platform.

**Examples**

```
nx9500-6C874D(config)#show raid
Logical drive info:
  Size 930 GB, State optimal
  Alarm enabled
  Last check: Sat Aug 10 02:56:54 2014
  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.

The system maintains a couple of default profiles. The default profile is automatically applied to service platforms and wireless controllers. The default AP profile is applied to an AP automatically discovered by a wireless controller or service platform. After adoption, if a change is made in one of the parameters in the profile, it is 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 are manually created for each supported service platform, wireless controller, and access point model. It is recommended that user-defined profiles 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
- AP6552 – Adds an AP6552 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
• AP81XX – Adds an AP81XX access point profile supporting the AP8122 and AP8132 models
• AP82XX – Adds an AP82XX access point profile supporting the AP8222 and AP8232 models
• 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
• NX65XX – Adds an NX65XX series service platform profile supporting the NX6500 and NX6524 models
• NX75XX – Adds an NX75XX series service platform profile supporting the NX7500 model
• NX9XXX – Adds an NX9XXX series service platform profile supporting the NX9000, NX9500, NX9600, and NX9510 models

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

To view the list of device profiles supported, use the following command:

<DEVICE>(config)#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
ap81xx   AP81XX access point profile
ap82xx   AP82XX access point profile
ap7502   AP7502 access point profile
ap7522   AP7522 access point profile
ap7532   AP7532 access point profile
containing Specify profiles that contain a sub-string in the profile name
filter    Specify addition selection filter
nx45xx   NX45XX integrated services platform profile
nx65xx   NX65XX integrated services platform profile
nx75xx   NX75XX wireless controller profile
nx9000   NX9000 wireless controller profile
rfs4000  RFS4000 wireless controller profile
rfs6000  RFS6000 wireless controller profile
rfs7000  RFS7000 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 ?
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
ap81xx AP81XX access point profile
ap82xx AP82XX access point profile

 nx4500-5CFA2B(config)#
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<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
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
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)
critical-resource Critical Resource
crypto Encryption related commands
device-upgrade Device firmware upgrade
dot1x 802.1X
dscp-mapping Configure IP DSCP to 802.1p priority mapping for untagged frames
dns-server
email-notification Email notification configuration
enforce-version Check the firmware versions of
environmental-sensor

devices before interoperating

environmental-sensor

Environment Sensors Configuration

events

System event messages

export

Export a file

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)

l2tpv3

L2tpv3 protocol

l3e-lite-table

L3e lite Table

led

Configure the time for the led to turn off after the last radio state change

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

Check controller connectivity after configuration is received

neighbor-inactivity-timeout

Configure neighbor inactivity timeout

neighbor-info-interval

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

remove-override

Remove configuration item override from the device (so profile value takes effect)

raid

RAID

rf-domain-manager

RF Domain Manager

router

Dynamic routing

slot

PCI expansion Slot

spanning-tree

Spanning tree

tunnel-controller

Tunnel Controller group this controller belongs to

use

Set setting to use

tunnel-controller

Tunnel Controller group this controller belongs to

vrrp

VRRP configuration

wep-shared-key-auth

Enable support for 802.11 WEP shared key authentication
clrscrn  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>)#
# 7.1 Profile Config Commands

Table 7.1 summarizes profile configuration 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 7-10</td>
</tr>
<tr>
<td>adoption</td>
<td>Configures adoption time delay settings</td>
<td>page 7-11</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, network-group, network-service, VLAN, and string aliases on this profile</td>
<td>page 7-12</td>
</tr>
<tr>
<td>ap300</td>
<td>Enables adoption of AP300s</td>
<td>page 7-18</td>
</tr>
<tr>
<td>area</td>
<td>Sets the system’s area of location (the area name)</td>
<td>page 7-19</td>
</tr>
<tr>
<td>arp</td>
<td>Configures static address resolution protocol</td>
<td>page 7-20</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enables network configuration learning of devices</td>
<td>page 7-22</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 7-23</td>
</tr>
<tr>
<td>autoinstall</td>
<td>Configures the automatic install feature</td>
<td>page 7-25</td>
</tr>
<tr>
<td>bluetooth-detection</td>
<td>Detects bluetooth devices using USB module</td>
<td>page 7-26</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures bridge specific parameters</td>
<td>page 7-28</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures captive portal advanced Web page upload on a device profile</td>
<td>page 7-47</td>
</tr>
<tr>
<td>cdp</td>
<td>Enables Cisco Discovery Protocol (CDP) on a device</td>
<td>page 7-48</td>
</tr>
<tr>
<td>cluster</td>
<td>Configures a cluster name</td>
<td>page 7-49</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enables persistence of configuration across reloads</td>
<td>page 7-51</td>
</tr>
<tr>
<td>controller</td>
<td>Configures a wireless controller or service platform</td>
<td>page 7-52</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Monitors user configured IP addresses and logs their status</td>
<td>page 7-55</td>
</tr>
<tr>
<td>crypto</td>
<td>Configures data encryption related protocols and settings</td>
<td>page 7-58</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings on this profile</td>
<td>page 7-119</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures 802.1x standard authentication controls</td>
<td>page 7-122</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configures an IP DSCP to 802.1p priority mapping for untagged frames</td>
<td>page 7-124</td>
</tr>
<tr>
<td>email-notification</td>
<td>Configures e-mail notification</td>
<td>page 7-125</td>
</tr>
</tbody>
</table>
**Table 7.1 Profile-Config Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enforce-version</code></td>
<td>Enables checking of a device’s firmware version before attempting adoption or clustering</td>
<td>page 7-127</td>
</tr>
<tr>
<td><code>environmental-sensor</code></td>
<td>Configures the environmental sensor settings on this profile</td>
<td>page 7-128</td>
</tr>
<tr>
<td><code>events</code></td>
<td>Displays system event messages</td>
<td>page 7-130</td>
</tr>
<tr>
<td><code>export</code></td>
<td>Enables export of startup.log file after every boot</td>
<td>page 7-131</td>
</tr>
<tr>
<td><code>floor</code></td>
<td>Sets the floor name where the system is located</td>
<td>page 7-132</td>
</tr>
<tr>
<td><code>gre</code></td>
<td>Enables <em>Generic Routing Encapsulation</em> (GRE) tunneling on this profile</td>
<td>page 7-133</td>
</tr>
<tr>
<td><code>http-analyze</code></td>
<td>Configures HTTP analysis settings</td>
<td>page 7-144</td>
</tr>
<tr>
<td><code>http-analyze</code> <em>(NX45XX, NX65XX, and NX9000)</em></td>
<td>Configures HTTP analysis settings on a NX series service platform (NX45XX, NX65XX, and NX9000)</td>
<td>page 7-145</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Configures an interface (VLAN, radio, GE etc.)</td>
<td>page 7-148</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Configures IP components</td>
<td>page 7-302</td>
</tr>
<tr>
<td><code>l2tpv3</code></td>
<td>Defines the <em>Layer 2 Tunnel Protocol</em> (L2TP) protocol for tunneling layer 2 payloads using <em>Virtual Private Networks</em> (VPNs)</td>
<td>page 7-311</td>
</tr>
<tr>
<td><code>l3e-lite-table</code></td>
<td>Configures L3e Lite Table with this profile</td>
<td>page 7-313</td>
</tr>
<tr>
<td><code>led</code></td>
<td>Turns device LEDs on or off</td>
<td>page 7-314</td>
</tr>
<tr>
<td><code>led-timeout</code></td>
<td>Configures LED-timeout timer. This command is specific to the NX9000 series service platforms.</td>
<td>led-timeout</td>
</tr>
<tr>
<td><code>legacy-auto-downgrade</code></td>
<td>Auto downgrades a legacy device firmware</td>
<td>page 7-316</td>
</tr>
<tr>
<td><code>legacy-auto-update</code></td>
<td>Auto upgrades a legacy device firmware</td>
<td>page 7-317</td>
</tr>
<tr>
<td><code>lldp</code></td>
<td>Configures <em>Link Layer Discovery Protocol</em> (LLDP)</td>
<td>page 7-318</td>
</tr>
<tr>
<td><code>load-balancing</code></td>
<td>Configures load balancing parameters</td>
<td>page 7-319</td>
</tr>
<tr>
<td><code>logging</code></td>
<td>Modifies message logging</td>
<td>page 7-324</td>
</tr>
<tr>
<td><code>mac-address-table</code></td>
<td>Configures the MAC address table</td>
<td>page 7-326</td>
</tr>
<tr>
<td><code>mac-auth</code></td>
<td>Enables 802.1x user authentication protocol on this profile</td>
<td>page 7-328</td>
</tr>
<tr>
<td><code>memory-profile</code></td>
<td>Configures the memory profile used on the device</td>
<td>page 7-331</td>
</tr>
<tr>
<td><code>meshpoint-device</code></td>
<td>Configures a meshpoint device parameters</td>
<td>page 7-333</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configures meshpoint monitoring interval</td>
<td>page 7-333</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Configures the minimum device connectivity verification time</td>
<td>page 7-334</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol</td>
<td>page 7-341</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Verifies device connectivity after a configuration is received</td>
<td>page 7-341</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configures neighbor inactivity timeout</td>
<td>page 7-342</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configures neighbor information exchange interval</td>
<td>page 7-343</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 7-344</td>
</tr>
<tr>
<td>noc</td>
<td>Configures NOC settings</td>
<td>page 7-347</td>
</tr>
<tr>
<td>ntp</td>
<td>Configures an NTP server</td>
<td>page 7-348</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 7-350</td>
</tr>
<tr>
<td>power-config</td>
<td>Configures the power mode</td>
<td>page 7-351</td>
</tr>
<tr>
<td>preferred-controller-group</td>
<td>Specifies the wireless controller or service platform group preferred for adoption</td>
<td>page 7-353</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 7-354</td>
</tr>
<tr>
<td>radius</td>
<td>Configures device-level RADIUS authentication parameters</td>
<td>page 7-355</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes the offline-duration settings applied at the device level</td>
<td>page 7-356</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 7-411</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Enables RF Domain manager</td>
<td>page 7-357</td>
</tr>
<tr>
<td>router</td>
<td>Configures dynamic router protocol settings</td>
<td>page 7-358</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Configures spanning tree commands</td>
<td>page 7-359</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Configures the name of tunneled WLAN (extended VLAN) wireless controller or service platform</td>
<td>page 7-362</td>
</tr>
<tr>
<td>use</td>
<td>Uses pre configured policies with this profile</td>
<td>page 7-363</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configures Virtual Router Redundancy Protocol (VRRP) group settings</td>
<td>page 7-367</td>
</tr>
</tbody>
</table>
Table 7.1 Profile-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wep-shared-key-auth</code></td>
<td>Enables support for 802.11 WEP shared key authentication</td>
<td>page 7-371</td>
</tr>
<tr>
<td><code>slot</code></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 7-376</td>
</tr>
</tbody>
</table>
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

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
use-adopter-auto-provisioning-policy-lookup

Parameters
None

Examples
rfs4000-229D58(config-profile-testRFS4000)#adopter-auto-provisioning-policy-lookup
rfs4000-229D58(config-profile-testRFS4000)#

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
  bridge vlan 1
    tunnel-over-level2
    ip igmp snooping
    ip igmp snooping querier
    no autoinstall configuration
    no autoinstall firmware
    device-upgrade persist-images
    .........................
    qos trust 802.1p
    interface ge4
      ip dhcp trust
      qos trust dscp
      qos trust 802.1p
    interface ge5
      ip dhcp trust
      qos trust dscp
      qos trust 802.1p
    interface wwan1
    interface pppoe1
    use firewall-policy default
    service pm sys-restart
    use-adopter-auto-provisioning-policy
    rfs4000-229D58(config-profile-testRFS4000)#

Related Commands

no
Removes the use of centralized auto provisioning policy on this profile or device
7.1.2 adoption

Profile Config Commands

Configures adoption time delay settings

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

adoption start-delay min <0-30> max <0-30>

Parameters

- adoption start-delay min <0-30> max <0-30>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adoption start-delay min &lt;0-30&gt; max &lt;0-30&gt;</td>
<td>Configures the time delay, an AP uses before starting an adoption attempt to be controlled.</td>
</tr>
<tr>
<td>&lt;start-delay&gt; min &lt;0-30&gt;</td>
<td>Specify the minimum delay time between 0 and 30 seconds.</td>
</tr>
<tr>
<td>max &lt;0-30&gt;</td>
<td>Specify the maximum delay time between 0 and 30 seconds.</td>
</tr>
</tbody>
</table>

Note: The minimum delay time is 5 seconds and maximum delay time is 20 seconds.

Examples

rfs6000-81742D(config-profile-default-rfs6000)#adoption start-delay min 5 max 10
rfs6000-81742D(config-profile-default-rfs6000)#

Related Commands

- no | Removes the adoption configuration settings |
### 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 be 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX7522, NX81XX, NX82XX

**Syntax**

```plaintext
alias [address-range|bonjour-service|host|network|network-group|network-service|string|vlan]
alias bonjour-service <BONJOUR-SERVICE-ALIAS-NAME>  <SERVICE-STRING>
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>]
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 string <STRING-ALIAS-NAME> <LINE>
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

**Parameters**

- **alias bonjour-service <BONJOUR-SERVICE-ALIAS-NAME> <SERVICE-STRING>**
  
  **bonjour-service <BONJOUR-SERVICE-ALIAS-NAME>**
  
  Creates a Bonjour service alias, which maps a user-friendly to a service
  
  **<BONJOUR-SERVICE-ALIAS-NAME>** — Specify the alias name. Use a user-friendly name that enables you to easily identify the associated Bonjour service.
  
  For example, _home-sharing._tcp.local can be mapped to $homeshare.
  
  **Note:** Alias name should begin with `$`.

  **<SERVICE-STRING>**
  
  Specify the RFC name of the Bonjour service.
  
  **Note:** This bonjour-service alias can be used in a bonjour-gw-discovery-policy. For more information, see bonjour-gw-discovery-policy.
• alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>

address-range <ADDRESS-RANGE-ALIAS-NAME> 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.

• <ADDRESS-RANGE-ALIAS-NAME> – Specify the address range alias name.

Note: Alias name should begin with '$'.

<STARTING-IP> to <ENDING-IP> Associates a range of IP addresses with this address range alias

• <STARTING-IP> – Specify the first IP address in the range.
• to <ENDING-IP> – Specify the last IP address in the range.

Note: If using an existing address-range alias, you can apply overrides to the alias at the profile level.

• alias host <HOST-ALIAS-NAME> <HOST-IP>

host <HOST-ALIAS-NAME> Creates a new host alias for this profile. Or associates an existing host alias with this profile. A host alias maps a name to a single network host.

• <HOST-ALIAS-NAME> – Specify the host alias name.

Note: Alias name should begin with '$'.

<HOST-IP> Associates the network host's IP address with this host alias

• <HOST-IP> – Specify the network host's IP address.

Note: If using an existing host alias, you can apply overrides to the alias at the profile level.

• alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

network <NETWORK-ALIAS-NAME> Creates a new network alias for this profile. Or associates an existing network alias with this profile. A network alias maps a name to a single network address.

• <NETWORK-ALIAS-NAME> – Specify the network alias name.

Note: Alias name should begin with '$'.

<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.

• alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> | host <HOST-IP> | network <NETWORK-ADDRESS/MASK>]

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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-range</code></td>
<td>Associates a range of IP addresses with this network-group alias.</td>
</tr>
<tr>
<td><code>&lt;STARTING-IP&gt;</code></td>
<td>Specify the first IP address in the range.</td>
</tr>
<tr>
<td>to <code>&lt;ENDING-IP&gt;</code></td>
<td>Specify the last IP address in the range.</td>
</tr>
<tr>
<td><code>{&lt;STARTING-IP&gt;</code></td>
<td>Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.</td>
</tr>
<tr>
<td><code>host &lt;HOST-IP&gt;</code></td>
<td>Associates a single or multiple hosts with this network-group alias.</td>
</tr>
<tr>
<td><code>{&lt;HOST-IP&gt;}</code></td>
<td>Specify the hosts’ IP address.</td>
</tr>
<tr>
<td><code>{&lt;HOST-IP&gt;}</code></td>
<td>Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.</td>
</tr>
<tr>
<td><code>network &lt;NETWORK-ADDRESS/MASK&gt;</code></td>
<td>Associates a single or multiple networks with this network-group alias.</td>
</tr>
<tr>
<td><code>{&lt;NETWORK-ADDRESS/MASK&gt;}</code></td>
<td>Specify the network’s address and mask.</td>
</tr>
<tr>
<td><code>{&lt;NETWORK-ADDRESS/MASK&gt;}</code></td>
<td>Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.</td>
</tr>
</tbody>
</table>

- `alias network-service <NETWORK-SERVICE-ALIAS-NAME>`
  - Creates a new network-service alias for this profile. Or associates an existing network-service alias with this profile. 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:** 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.
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).
- 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 string <STRING-ALIAS-NAME> <LINE>

**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. For example, alias string `$DOMAIN test.company.com`. In this example, the string alias name is: `$DOMAIN` and the string value it is mapped to is: `test.company.com`. In this example, the string alias refers to a domain name.

- `<VLAN-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>

<table>
<thead>
<tr>
<th>alias vlan &lt;VLAN-ALIAS-NAME&gt;</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;VLAN-ALIAS-NAME&gt; – Specify the VLAN alias name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Alias name should begin with '$'.</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>Maps the VLAN alias to a VLAN ID</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If using an existing VLAN alias, you can apply overrides to the alias at the profile level.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows the global aliases configured. Note the network-service alias '$kerberos' settings.

```
    rfs4000-229D58(config)#show context
        !
        ! Configuration of RFS4000 version 5.5.6.0-006D
        !
        ! 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:

```
    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:
rfs4000-229D58(config-profile-TestRFS4000)#show context
profile rfs4000 TestRFS4000
  no autoinstall configuration
  no autoinstall firmware
 ...............................................................
  interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  interface wwan1
  interface pppoe1
  use firewall-policy default
  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><code>no</code></td>
<td>Removes the use of centralized auto provisioning policy on this profile or device</td>
</tr>
</tbody>
</table>
7.1.4 ap300

Profile Config Commands

Enables or disables adoption of an AP300 by devices using this profile

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000, NX9500, NX9510, NX9600

Syntax

ap300 [ <MAC> | adopt-unconfigured ]
ap300 <MAC> [ adopt | deny ]
ap300 adopt-unconfigured

Parameters

- ap300 <MAC> [ adopt | deny ]
- ap300 adopt-unconfigured

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#ap300 00-15-70-63-4F-86 adopt
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping querier
  ip igmp snooping querier
  arp timeout 2000
  crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
  qos trust 802.1p
  interface pppoe1
  --More--
  use firewall-policy default
  ap300 00-15-70-63-4F-86 adopt
  service pm sys-restart
  router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

no

Dissociates (unmaps) an AP300 from the adopt or deny list. Also disables non-configured AP300 adoption.
### 7.1.5 area

#### Profile Config Commands

Sets the system’s area of location (the area name)

Supported in the following platforms:

- **Access Points** — AP300, 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, 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       
profile rfs7000 default-rfs7000
  bridge vlan 1
  ip igmp snooping
  ip igmp snooping querier
  area Ecospace
  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
  --More--
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#
```

#### Related Commands

```
no
```

Resets the configured area name
### 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
arp [ <IP> | timeout ]
```

```
arp <IP> <MAC> arpa [ <L3-INTERFACE-NAME> | pppoe1 | vlan <1-4094> | wwan1 | serial <1-4> ] { dhcp-server | router }
```

```
arp timeout <15-86400>
```

**Parameters**

- `arp <IP> <MAC> arpa [ <L3-INTERFACE-NAME> | pppoe1 | vlan <1-4094> | wwan1 | serial <1-4> ] { dhcp-server | router }`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arp &lt;IP&gt;</code></td>
<td>Adds a static ARP IPv4 address in the ARP cache.</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Specify the static IP address.</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>Specify the MAC address associated with the IP and the Switch Virtual Interface (SVI).</td>
</tr>
<tr>
<td><code>arpa</code></td>
<td>Sets ARP encapsulation type to ARPA.</td>
</tr>
<tr>
<td><code>&lt;L3-INTERFACE-NAME&gt;</code></td>
<td>Configures static ARP entry for a specified router interface.</td>
</tr>
<tr>
<td><code>&lt;1-1&gt;</code></td>
<td>Specify the router interface name.</td>
</tr>
<tr>
<td><code>pppoe1</code></td>
<td>Configures static ARP entry for PPP over Ethernet interface.</td>
</tr>
<tr>
<td><code>vlan &lt;1-4094&gt;</code></td>
<td>Configures static ARP entry for a VLAN interface.</td>
</tr>
<tr>
<td><code>&lt;1-4094&gt;</code></td>
<td>Specify a SVI VLAN ID from 1 - 4094.</td>
</tr>
<tr>
<td><code>wwan1</code></td>
<td>Configures static ARP entry for Wireless WAN interface.</td>
</tr>
<tr>
<td><code>serial &lt;1-4&gt;</code></td>
<td>Configures the static ARP entry for serial interface.</td>
</tr>
<tr>
<td><code>&lt;1-4&gt;</code></td>
<td>Specify the Slot ID.</td>
</tr>
<tr>
<td><code>&lt;1-1&gt;</code></td>
<td>Specify the port ID.</td>
</tr>
<tr>
<td><code>&lt;1-1&gt;</code></td>
<td>Specify the Channel group ID.</td>
</tr>
</tbody>
</table>

The serial interface is applicable for the NX45XX and NX65XX series service platforms only.
### arp timeout <15-86400>

Sets ARP entry timeout

- **<TIME>** – Sets the ARP entry timeout in seconds. Specify a value from 15 - 86400 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 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 me1
  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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes an entry from the ARP cache</td>
</tr>
</tbody>
</table>
7.1.7 auto-learn-staging-config

Profile Config Commands

Enables automatic recognition of devices pending adoption

Supported in the following platforms:

- Access Points — AP300, 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, 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. These substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for a 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: TestAP6522\textit{B4C7996C8809}. 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`autogen-uniqueid <WORD>`

**Parameters**

- `autogen-uniqueid <WORD>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>autogen-uniqueid &lt;WORD&gt;</code></td>
<td>Autogenerates a device’s unique ID (not exceeding 64 characters in length)</td>
</tr>
<tr>
<td></td>
<td>The ID generated is a combination of the text provided and 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.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;WORD&gt;</code> – Specify a auto generate unique ID format using one of the following substitution tokens:</td>
</tr>
<tr>
<td></td>
<td>- Available tokens:</td>
</tr>
<tr>
<td></td>
<td>- $SN - references SERIAL NUMBER of the device</td>
</tr>
<tr>
<td></td>
<td>- $MiNT-ID - references MiNT-ID of the device</td>
</tr>
<tr>
<td></td>
<td>For example, ORG-$SN-DEPT, In this example ‘ORG’ and ‘DEPT’ represent the user-defined prefix and suffix respectively. And $SN is the substitution token.</td>
</tr>
</tbody>
</table>
Examples

```
x4500-5CFA2B(config-profile-testAP6522)#autogen-uniqueid TestAP6522$SN
```

```
x4500-5CFA2B(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)#
```

```
x4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#autogen-uniqueid Test-$MiNT-ID-TechPubs
```

```
x4500-5CFA2B(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

```
no
```

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.
7.1.9 autoinstall

Profile Config Commands

Automatically installs firmware image and configuration parameters on to the selected device.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

autoinstall [configuration|firmware|start-interval <WORD>]

Parameters

- autoinstall [configuration|firmware|start-interval <WORD>]

<table>
<thead>
<tr>
<th>Parameters</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</td>
</tr>
<tr>
<td>firmware</td>
<td>Autoinstalls firmware image. Firmware images are automatically installed on devices using this profile</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.</td>
</tr>
</tbody>
</table>

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
  --More--
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

- **no** Disables the auto install settings
### 7.1.10 bluetooth-detection

#### Profile Config Commands

Detects bluetooth devices using the bluetooth USB module

Supported in the following platforms:
- Access Points — AP81XX

#### Syntax

```
bluetooth-detection
```

#### Parameters

None

#### Examples

```
rfs6000-81742D(config-profile-default-rfs6000)#bluetooth-detection
%Error: device type rfs6000 does not support bluetooth-detection
rfs6000-81742D(config-profile-default-rfs6000)#
```
7.1.11 bridge

Profile Config Commands

Table 7.2 summarizes Ethernet bridge configuration commands.

Table 7.2 Bridge-Config 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 7-28</td>
</tr>
<tr>
<td>bridge-vlan-mode commands</td>
<td>Summarizes bridge VLAN configuration mode commands</td>
<td>page 7-31</td>
</tr>
</tbody>
</table>
7.1.11.1 bridge

Configure 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Switch Note:** The interfaces mentioned below are supported as follows:
- ge <index> – RFS7000 and RFS4000 supports 4 GEs, AP621 supports 8 GEs, NX45XX and NX65XX supports 24 GEs
- me1 – Only supported on RFS7000 and RFS6000

**Syntax**

```plaintext
bridge [nat|vlan]

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>}>]

bridge vlan <1-4095>
```
### 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>)]
  - `nat`: Configures bridge NAT parameters
  - `source`: Configures NAT source addresses
  - `list <IP-ACCESS-LIST-NAME> precedence <1-500>`: 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.
    - `<IP-ACCESS-LIST-NAME>` – Specify access list name.
    - `precedence <1-500>` – Specifies a precedence value for this bridge NAT policy.
  - `interface [<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1]`: Selects one of the following as the primary interface (between the source and destination points):
    - `<LAYER3-INTERFACE-NAME>` – A router interface. Specify interface name.
    - `pppoe1` – A PPP over Ethernet interface
    - `vlan <1-4094>` – A VLAN interface. Specify the VLAN interface index from 1 - 4094.
    - `wwan1` – A Wireless WAN interface
  - `[(address|interface|overload|pool <NAT-POOL-NAME>)]`: The following keywords are recursive and common to all interface types:
    - `address`: Configures the interface IP address used for NAT
    - `interface`: Configures the failover interface (default setting)
    - `overload`: Enables use of one global address for multiple local addresses (terminates command)
    - `pool <NAT-POOLNAME>`: Configures the NAT pool used with this bridge NAT policy. Specify the NAT pool name. For more information on configuring a NAT pool, see [nat-pool-config-instance](#).

- **bridge vlan <1-4095>**
  - `vlan <1-4095>`: Configures the numerical identifier for the Bridge VLAN when it was initially created.
    - `<1-4095>` – Specify a VLAN index from 1 - 4095.

### 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.
- **description**: Vlan description.
- **edge-vlan**: Enable edge-VLAN mode.
- **firewall**: Enable vlan firewall.
- **ip**: Internet Protocol (IP).
- **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)#
7.1.11.2 bridge-vlan-mode commands

Table 7.3 summarizes bridge VLAN configuration mode commands.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bridging-mode</strong></td>
</tr>
<tr>
<td>Configures how packets on this VLAN are bridged</td>
</tr>
<tr>
<td><strong>description</strong></td>
</tr>
<tr>
<td>Configures VLAN bridge description</td>
</tr>
<tr>
<td><strong>edge-vlan</strong></td>
</tr>
<tr>
<td>Enables edge VLAN mode</td>
</tr>
<tr>
<td><strong>firewall</strong></td>
</tr>
<tr>
<td>Enables VLAN fire wall</td>
</tr>
<tr>
<td><strong>ip</strong></td>
</tr>
<tr>
<td>Configures IP components</td>
</tr>
<tr>
<td><strong>l2-tunnel-broadcast-optimization</strong></td>
</tr>
<tr>
<td>Enables broadcast optimization</td>
</tr>
<tr>
<td><strong>no</strong></td>
</tr>
<tr>
<td>Negates a command or reverts settings to their default</td>
</tr>
<tr>
<td><strong>stateful-packet-inspection-l2</strong></td>
</tr>
<tr>
<td>Enables stateful packet inspection in the layer 2 fire wall</td>
</tr>
<tr>
<td><strong>tunnel</strong></td>
</tr>
<tr>
<td>Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge</td>
</tr>
<tr>
<td><strong>tunnel-over-level2</strong></td>
</tr>
<tr>
<td>Enables extended VLAN traffic over level 2 MiNT links</td>
</tr>
<tr>
<td><strong>use</strong></td>
</tr>
<tr>
<td>Uses pre configured access lists with this PF bridge policy</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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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 (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, are 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**

```bash
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#bridging-mode isolated-tunnel
```

```bash
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
```

**Related Commands**

- `no` | Resets bridging mode to auto
**7.1.11.2.2 description**

> **bridge-vlan-mode commands**

Configures VLAN bridge description

Supported in the following platforms:

- Access Points — AP300, 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, 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 VLAN bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WORD&gt; – Specify VLAN description. The description should be unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.</td>
<td></td>
</tr>
</tbody>
</table>

**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
7.1.11.2.3 edge-vlan

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 enabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
edge-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><strong>no</strong></td>
<td>Disables the edge VLAN mode</td>
</tr>
</tbody>
</table>
7.1.11.2.4 firewall

- bridge-vlan-mode commands

Enables firewall on this VLAN interface. This feature is enabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, 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>no</td>
<td>Disables a VLAN's firewall</td>
</tr>
</tbody>
</table>
### 7.1.11.2.5 `ip`

#### bridge-vlan-mode commands

Configures VLAN bridge IP components

Supported in the following platforms:
- **Access Points** — AP300, 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, 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 {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

- **ip [arp|dhcp] trust**
  - Configures the VLAN bridge IP parameters
  - `arp trust` Configures the ARP trust parameter. Trusted ARP packets are used to update the DHCP snoop table to prevent IP spoof and arp-cache poisoning attacks. This option is disabled by default.
    - trust – Trusts ARP responses on the VLAN bridge
  - `dhcp trust` 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 snoop table to prevent IP spoof attacks. This feature is disabled by default.
    - trust – Trusts DHCP responses on the VLAN bridge
- **ip igmp snooping {forward-unknown-multicast}
  - Configures the VLAN bridge IP parameters
  - `igmp snooping` Configures Internet Group Management Protocol (IGMP) snooping parameter
    - The IGMP protocol 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.
    - `forward-unknown-multicast` 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 disabled by default.
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}

- `ip` Configures the VLAN bridge IP parameters
- `igmp snooping` Configures the IGMP snooping parameters
- `mrouter` Optional. Configures the multicast router parameters
  - `<INTERFACE-LIST>` – Specify a comma-separated list of interface names.
- `learn pim-dvmrp` Configures the multicast router learning protocols
  - `pim-dvmrp` – Enables Protocol-Independent Multicast (PIM) and Distance-Vector Multicast Routing Protocol (DVMRP) snooping of packets

ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|timer expiry <60-300>|version <1-3>}

- `ip` Configures the VLAN bridge IP parameters
- `igmp snooping` Configures the IGMP snooping parameters
- `querier` Optional. Configures the IGMP querier parameters
  - Enables IGMP querier. IGMP snoop 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.
- `address <IP>` Optional. Configures the IGMP querier source IP address
  - `<IP>` – Specify the IGMP querier source IP address.
- `max-response-time <1-25>` Optional. Configures the IGMP querier maximum response time
  - `<1-25>` – Specify the maximum response time from 1 - 25 seconds. The default is 10 seconds.
  - The access point, wireless controller, or service platform forwards multicast packets only to radios present in the snooping table. IGMP reports from wired ports are forwarded to the multicast router ports.
  - If no reports are received from a radio, it is removed from the snooping table. The radio then stops receiving multicast packets.
- `timer expiry <60-300>` Optional. Configures the IGMP querier timeout
  - `expiry` – Configures the IGMP querier timeout
  - `<60-300>` – Specify the IGMP querier timeout from 60 - 300 seconds.
- `version <1-3>` Optional. Configures the IGMP version
  - `<1-3>` – Specify the IGMP version. The versions are 1-3. The default is 3.
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-dvmrp
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ridge 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>
7.1.11.2.6 l2-tunnel-broadcast-optimization

- **bridge-vlan-mode commands**

Enables broadcast optimization on this VLAN interface. Enabling this feature aids in the identification of each incoming packet. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
l2-tunn2l-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>
### 7.1.11.2.7 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

- `no [bridging-mode|description|edge-vlan|firewall|ip|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-level12]`
- `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 tunnel unknown-unicast`
- `no use [ip-access-list|mac-access-list] tunnel out`

#### Parameters

- `no [bridging-mode|description|edge-vlan|firewall|l2-tunnel-broadcast-optimization|stateful-packet-inspection-12|tunnel-over-level2]`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no bridging-mode</code></td>
<td>Resets the bridging mode to ‘auto’</td>
</tr>
<tr>
<td><code>no description</code></td>
<td>Removes the VLAN’s description</td>
</tr>
<tr>
<td><code>no edge-vlan</code></td>
<td>Disables the edge VLAN mode</td>
</tr>
<tr>
<td><code>no firewall</code></td>
<td>Disables the VLAN’s firewall</td>
</tr>
<tr>
<td><code>no l2-tunnel-broadcast-optimization</code></td>
<td>Disables broadcast optimization</td>
</tr>
<tr>
<td><code>no tunnel-over-level2</code></td>
<td>Disables extended VLAN traffic over level 2 MiNT links</td>
</tr>
<tr>
<td><code>no stateful-packet-inspection-12</code></td>
<td>Disables state packet inspection in the layer 2 firewall</td>
</tr>
</tbody>
</table>
- `no ip [arp|dhcp] trust`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no ip</code></td>
<td>Negates or reverts VLAN bridge IP settings</td>
</tr>
<tr>
<td><code>arp trust</code></td>
<td>Disables the trust of ARP responses on the VLAN</td>
</tr>
<tr>
<td><code>dhcp trust</code></td>
<td>Disables the trust of DHCP responses on the VLAN</td>
</tr>
</tbody>
</table>
### Profile Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no ip igmp snooping {forward-unknown-multicast}</code></td>
<td>Negates or reverts the VLAN bridge IP settings</td>
</tr>
<tr>
<td><code>no ip igmp snooping</code></td>
<td>Negates or reverts the IGMP snooping settings</td>
</tr>
<tr>
<td><code>forward-unknown-multicast</code></td>
<td>Optional. Disables the forwarding of unknown multicast packets</td>
</tr>
<tr>
<td>`no ip igmp snooping {mrouter [interface &lt;INTERFACE-LIST&gt;</td>
<td>learn pim-dvmrp]}`</td>
</tr>
<tr>
<td><code>igmp snooping</code></td>
<td>Negates or reverts the IGMP snooping settings</td>
</tr>
<tr>
<td><code>mrouter</code></td>
<td>Optional. Resets or disables multicast router parameters</td>
</tr>
<tr>
<td><code>interface &lt;INTERFACE-LIST&gt;</code></td>
<td>Optional. Disables mrouter interfaces</td>
</tr>
<tr>
<td><code>learn pim-dvmrp</code></td>
<td>Optional. Disables multicast router learning protocols</td>
</tr>
<tr>
<td>`no ip igmp snooping {querier {address</td>
<td>max-response-time</td>
</tr>
<tr>
<td><code>igmp snooping</code></td>
<td>Negates the IGMP snooping components</td>
</tr>
<tr>
<td><code>querier</code></td>
<td>Optional. Disables the IGMP querier</td>
</tr>
<tr>
<td><code>address</code></td>
<td>Optional. Reverts to the default IGMP querier source IP address of 0.0.0.0</td>
</tr>
<tr>
<td><code>max-response-time</code></td>
<td>Optional. Reverts to the default IGMP querier maximum response time</td>
</tr>
<tr>
<td><code>timer expiry</code></td>
<td>Optional. Reverts to the default IGMP querier timeout</td>
</tr>
<tr>
<td><code>version &lt;1-3&gt;</code></td>
<td>Optional. Reverts to the default IGMP version</td>
</tr>
<tr>
<td><code>no tunnel unknown-unicast</code></td>
<td>Enables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge</td>
</tr>
<tr>
<td>`no use [ap-access-list</td>
<td>mac-access-list] tunnel out`</td>
</tr>
<tr>
<td><code>ip-access-list tunnel out</code></td>
<td>Removes the VLAN bridge’s IP access list</td>
</tr>
<tr>
<td><code>mac-access-list tunnel out</code></td>
<td>Removes the VLAN bridge’s MAC access list</td>
</tr>
</tbody>
</table>

- **tunnel** – Prevents the IP access list from being applied to all packets going into a tunnel |
- **out** – Prevents the IP access list from being applied to all outgoing packets
**Examples**

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no description

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp snooping mrouter

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp snooping mrouter learn pim-dvmrp

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp snooping querier

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp snooping querier max-response-time

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#no ip igmp snooping querier version

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context bridge vlan 1

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context bridge vlan 1

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context bridge vlan 1

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context bridge vlan 1

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging-mode</td>
<td>Configures the VLAN’s bridging mode</td>
</tr>
<tr>
<td>description</td>
<td>Configures the VLAN’s description</td>
</tr>
<tr>
<td>edge-vlan</td>
<td>Enables the edge VLAN mode</td>
</tr>
<tr>
<td>ip</td>
<td>Configures the VLAN’s IP components</td>
</tr>
<tr>
<td>l2-tunnel-broadcast-optimization</td>
<td>Enables broadcast optimization</td>
</tr>
<tr>
<td>stateful-packet-inspection-l2</td>
<td>Enables stateful packet inspection in the layer 2 firewall</td>
</tr>
<tr>
<td>tunnel</td>
<td>Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge</td>
</tr>
<tr>
<td>tunnel-over-level2</td>
<td>Enables extended VLAN traffic over level 2 MiNT links</td>
</tr>
<tr>
<td>use</td>
<td>Uses pre configured access lists with this PF bridge policy</td>
</tr>
</tbody>
</table>
### 7.1.11.2.8 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** — AP300, 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, 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>no</td>
<td>Disables stateful packet inspection at the layer 2 firewall</td>
</tr>
</tbody>
</table>
7.1.11.2.9 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

tunnel unknown-unicast

**Parameters**

None

**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**

| **no** | Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge |
7.11.2.10 tunnel-over-level2

▶ bridge-vlan-mode commands

Enables extended VLAN (tunneled VLAN) traffic over level 2 MiNT links

Supported in the following platforms:

- Access Points — AP300, 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, 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables extended VLAN traffic over level 2 MiNT links</td>
</tr>
</tbody>
</table>
7.1.11.2.11 use

*bridge-vlan-mode commands*

Uses pre configured access lists with this bridge policy

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use [ip-access-list|mac-access-list] tunnel out <IP/MAC-ACCESS-LIST-NAME>
```

**Parameters**

- `use [ip-access-list|mac-access-list] tunnel out <IP/MAC-ACCESS-LIST-NAME>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>Sets this VLAN bridge policy to use an IP access list or a MAC access list</td>
</tr>
<tr>
<td>ip-access-list</td>
<td>Associates a pre-configured IP access list with this VLAN-bridge interface</td>
</tr>
<tr>
<td>mac-access-list</td>
<td>Uses a pre-configured MAC access list with this VLAN-bridge interface</td>
</tr>
<tr>
<td>tunnel out</td>
<td>The following keywords are common to the 'IP access list' and 'MAC access list' parameters:</td>
</tr>
<tr>
<td>&lt;IP/MAC-ACCESS-LIST-NAME&gt;</td>
<td>- tunnel — Applies IP access list or MAC access list to all packets going into the tunnel</td>
</tr>
<tr>
<td></td>
<td>- out — Applies IP access list or MAC access list to all outgoing packets</td>
</tr>
<tr>
<td></td>
<td>- &lt;IP/MAC-ACCESS-LIST-NAME&gt; — Specify the IP access list or MAC access list name.</td>
</tr>
</tbody>
</table>

**Examples**

```
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

captive-portal page-upload count <1-20>

Parameters

- captive-portal page-upload count <1-20>

<table>
<thead>
<tr>
<th>page-upload</th>
<th>Enables captive portal advanced Web page upload</th>
</tr>
</thead>
<tbody>
<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.</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

Uses *Cisco Discovery Protocol* (CDP) as a layer 2 protocol that discovers information about neighboring network devices.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```bash
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/disables 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 time between advertisements</td>
</tr>
</tbody>
</table>

#### Examples

```bash
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
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables CDP on this profile</td>
</tr>
</tbody>
</table>
### 7.1.14 cluster

#### Profile Config Commands

Sets the cluster configuration

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

cluster [force-configured-state|force-configured-state-delay|handle-stp|master-priority|member|mode|name]

cluster [force-configured-state|force-configured-state-delay <3-1800>|handle-stp|master-priority <1-255>]

custer member [ip|vlan]
custer member [ip <IP> {level [1|2]}|vlan <1-4094>]
custer mode [active|standby]
custer name <CLUSTER-NAME>

#### 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 active controller becomes active again.

- **handle-stp**
  - Enables/disables 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.

- **master-priority <1-255>**
  - 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.

- **member**
  - 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.

- **mode**
  - 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.

- **name <CLUSTER-NAME>**
  - 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.
### cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]

- **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.

### cluster mode [active|standby]

- **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.

### cluster name <CLUSTER-NAME>

- **name <CLUSTER-NAME>**
  - Configures the cluster name
  - `<CLUSTER-NAME>` – Specify the cluster name.

### 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
cluster name cluster1
cluster member ip 172.16.10.3
cluster member vlan 1
rfs7000-37FABE(config-profile-default-rfs7000)#`

### Related Commands

- `no`
  - Removes cluster member
7.1.15 configuration-persistence

Profile Config Commands

Enables configuration persistence across reloads

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP811X, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
configuration-persistence {secure}

Parameters
- configuration-persistence {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 4094
  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 WLAN's controller (wireless controller or service platform) settings

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

controller [adopted-devices|adoption|group|hello-interval|vlan|host]
controller adopted-devices [aps|controllers]
controller adopted-devices [aps {controllers}|controllers {aps}]
controller adoption
controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]
controller hello-interval <1-120> adjacency-hold-time <2-600>
controller host [<IP>|<HOSTNAME>] {ipsec-secure|level|pool|remote-vpn-client}
controller host [<IP>|<HOSTNAME>] level [1|2] pool <1-2> level [1|2] {ipsec-secure {gw}}
controller host [<IP>|<HOSTNAME>] remote-vpn-client

Parameters
- controller adopted-devices [aps {controllers}|controllers {aps}]

<table>
<thead>
<tr>
<th>controller</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the WLAN's controller settings</td>
<td></td>
</tr>
<tr>
<td>adopted-devices</td>
<td>Configures the types of device (AP/controller) this controller can adopt</td>
</tr>
<tr>
<td>aps {controllers}</td>
<td>Enables the adoption of access points by this controller. This is the default setting.</td>
</tr>
<tr>
<td>controllers – Optional. Enables the adoption of controllers by this controller</td>
<td></td>
</tr>
<tr>
<td>All adopted devices (referred to as adoptee) receive complete configuration from the adopting controller (referred to as adopter).</td>
<td></td>
</tr>
<tr>
<td>controllers {aps}</td>
<td>Enables the adoption of controllers by this controllers</td>
</tr>
<tr>
<td>aps – Optional. Enables the adoption of access points by this controller</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Use the no &gt; controller &gt; adopted-devices command to remove this setting.</td>
<td></td>
</tr>
</tbody>
</table>

- controller adoption

<table>
<thead>
<tr>
<th>controller adoption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables adoption of the logged wireless controller or service platform</td>
<td></td>
</tr>
<tr>
<td>Use the no &gt; controller &gt; adoption command to disable adoption.</td>
<td></td>
</tr>
</tbody>
</table>
- **controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]**

<table>
<thead>
<tr>
<th>controller</th>
<th>Configures the WLAN's controller settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>group &lt;CONTROLLER-GROUP-NAME&gt;</td>
<td>Configures the wireless controller or service platform group</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Configures the wireless controller or service platform VLAN</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>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>
</tbody>
</table>

- **controller host [<IP>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]} {ipsec-secure {gw}}**

<table>
<thead>
<tr>
<th>controller</th>
<th>Configures the WLAN's controller settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>host [&lt;IP&gt;</td>
<td>&lt;HOSTNAME&gt;]</td>
</tr>
<tr>
<td>level [1</td>
<td>2]</td>
</tr>
<tr>
<td>pool &lt;1-2&gt; level [1</td>
<td>2]</td>
</tr>
<tr>
<td>ipsec-secure {gw}</td>
<td>The following keywords are recursive and common to the ‘level’ and ‘pool’ parameters:</td>
</tr>
</tbody>
</table>
**controller host [<IP>|<HOSTNAME>] {remote-vpn-client}**

<table>
<thead>
<tr>
<th>controller</th>
<th>Configures the WLAN’s controller settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>host [&lt;IP&gt;</td>
<td>&lt;HOSTNAME&gt;]</td>
</tr>
<tr>
<td>remote-vpn-client</td>
<td>Forces MiNT link creation protocol (MLCP) to use remote VPN connection on the controller</td>
</tr>
</tbody>
</table>

- `<IP>` – Configures wireless controller or service platform’s IP address
- `<HOSTNAME>` – Configures wireless controller or service platform’s name

**Examples**

```plaintext
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
  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
      qos trust 802.1p
    interface ge2
      ip dhcp trust
      qos trust dscp
      qos 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
  use firewall-policy default
controller 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
critical-resource [monitor]
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 [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 [ge <1-4>|port-channel <1-2>]
 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 [ge <1-4>|port-channel <1-2>]}
- `critical-resource monitor interval <5-86400>

<table>
<thead>
<tr>
<th><strong>&lt;CRM-POLICY-NAME&gt;</strong></th>
<th>Creates a critical resource monitoring policy, identified by the <strong>&lt;CRM-POLICY-NAME&gt;</strong> keyword. Provide the CRM policy name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Enables critical resource(s) monitoring |</td>
</tr>
</tbody>
</table>
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.

The following keywords are common to the ‘all’ and ‘any’ parameters:

- **arp-only** – 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

---

<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>Monitors configured critical resource(s)</td>
</tr>
<tr>
<td>via</td>
<td>Specifies the interface or next-hop via which the ICMP pings should be sent</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;LAYER3-INTERFACE-NAME&gt;</td>
<td>Specify the layer 3 Interface name (router interface)</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Specifies PPP over Ethernet interface</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Specifies the wireless controller or service platform’s VLAN interface. Specify VLAN ID from 1 - 4094.</td>
</tr>
<tr>
<td>wwan1</td>
<td>Specifies Wireless WAN interface</td>
</tr>
</tbody>
</table>
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.

### Critical-Resource Monitor Interval

**critical-resource 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

```bash
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
6c781f42a3638757d8849c38268b4ea48e483e2f986ae392ebcdd6a8f6f309443e93ad3123c3d76
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

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#critical-resource test monitor direct all 192.168.13.10 arp-only vlan 1
```

### Keywords 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.
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. Table 7.4 summarizes crypto configuration commands.

Table 7.4 Crypto-Config-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 7-59</td>
</tr>
<tr>
<td>crypto-auto-ipsec-tunnel commands</td>
<td>Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration</td>
<td>page 7-65</td>
</tr>
<tr>
<td>crypto-ikev1/ikev2-policy commands</td>
<td>Configures crypto IKEv1/IKEv2 policy parameters</td>
<td>page 7-72</td>
</tr>
<tr>
<td>crypto-ikev1/ikev2-peer commands</td>
<td>Configures IKEv1 peer parameters</td>
<td>page 7-80</td>
</tr>
<tr>
<td>crypto-map-config-commands</td>
<td>Configures crypto map parameters</td>
<td>page 7-89</td>
</tr>
<tr>
<td>crypto-remote-vpn-client commands</td>
<td>Configures remote VPN client settings</td>
<td>page 7-114</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 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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-md5-hmac|esp-sha-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>auto-ipsec-secure</th>
<th>Configures the Auto IPSec Secure parameter settings. For Auto IPSec tunnel configuration commands, see crypto-auto-ipsec-tunnel commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>enable-ike-uniqueids</td>
<td>Enables Internet Key Exchange (IKE) unique ID check. For more information on IKE unique IDs, see <code>remotegw</code>.</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]`

- 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 <1-100>|nat-keepalive <10-3600>|peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]`

- ikev1 | Configures the IKEv1 parameters. |
- dpd-keepalive | Sets the global Dead Peer Detection (DPD) interval from 10 - 3600 seconds. |
- dpd-retries | Sets the global DPD retries count from 1 - 100. |
- nat-keepalive | Sets the global NAT keepalive interval from 10 - 3600 seconds. |
- peer | Specify the Name/Identifier for the IKEV1 peer. For IKEV1 peer configuration commands, see `crypto-ikev1/ikev2-peer commands`. |
- policy | 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`. |
- remote-vpn | Specifies the IKEV1 remote-VPN server configuration (responder only). |

**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]`

- ikev2 | Configures the IKEv2 parameters. |
- cookie-challenge-threshold | Starts cookie challenge after half open IKE SAs exceeds the specified limit. Sets the limit from 1 - 100. |
- dpd-keepalive | Sets the global DPD interval from 10 - 3600 seconds. |
- dpd-retries | Sets the global DPD retries count from 1 - 100. |
- nat-keepalive | Sets the global NAT keepalive interval from 10 - 3600 seconds. |
- peer | Specify the Name/Identifier for the IKEV2 peer. |
### Profiles

**policy**
- `<IKEV2-POLICY-NAME>`
  - Configures an ISKAMP policy. Specify the policy name. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations.

**remote-vpn**
- Specifies an IKEV2 remote-VPN server configuration (responder only)

---

### crypto ipsec

- `df-bit [clear|copy|set]`
  - Configures 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
    - `set` – Sets the DF bit in the outer header

---

### crypto ipsec security-association

- `lifetime [kilobytes <500-2147483646>|seconds <120-86400>]`
  - Defines the IPSec SAs lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds, whichever 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.
    - `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 security association lifetime can be overridden under crypto maps.

---

### crypto ipsec transform-set

- `<TRANSFORM-SET-TAG>`
  - Defines the transform set configuration (authentication and encryption) for securing data
    - `<TRANSFORM-SET-TAG>` – Specify the transform set name.
    - Specify the transform set used by the IPSec transport connection to negotiate the transform algorithm.

### esp-3des
- Configures the ESP transform using 3DES cipher (168 bits). The transform set is assigned to a crypto map using the map's set transform-set command.

### esp-aes
- Configures the ESP transform using Advanced Encryption Standard (AES) cipher. The transform set is assigned to a crypto map using the map's set transform-set command.

### esp-aes-192
- Configures the ESP transform using AES cipher (192 bits). The transform set is assigned to a crypto map using the map's set transform-set command.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 transform-set command.</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 transform-set command.</td>
</tr>
<tr>
<td>esp-null</td>
<td>Configures the ESP transform with no encryption</td>
</tr>
</tbody>
</table>
| {esp-md5-hmac, esp-sha-hmac} | The following keywords are common to all transform sets:  
| | • esp-md5-hmac – Configures ESP transform using HMAC-MD5 authorization  
| | • esp-sha-hmac – Configures ESP transform using HMAC-SHA authorization |

**Comments**

- `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 Commands](#).

- `<1-1000>` Defines the crypto map entry sequence. 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 CA certificate or both
  - `<TRUSTPOINT-NAME>` – Specify the trustpoint name.

- `<URL>` Specify the CRL source address in the following format:
  - tftp://<hostname>[port]/path/file
  - ftp://<user>:<passwd>@<hostname>[port]/path/file
  - sftp://<user>:<passwd>@<hostname>[port]/path/file
  - http://<hostname>[port]/path/file
  - cf:/path/file
  - usb<n>:/path/file

- `<1-168>` Sets command replay duration from 1 - 168 hours

- `crypto plain-text-deny-acl-scope [global | interface]`

- `plain-text-deny-acl-scope` Configures plain-text-deny-acl-scope parameters
### crypto remote-vpn-client

- **global**
  - Applies the plain text deny ACL globally

- **interface**
  - Applies the plain text deny ACL to the interface only

**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

<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>
### 7.18.2 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 tunneled 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 Security Associations (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).

Internet Key Exchange (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 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

- `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-crypto-auto-ipsec-secure)#
```

Table 7.5 summarizes the crypto IPSec auto tunnel 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 7-66</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 7-67</td>
</tr>
<tr>
<td><code>ike-lifetime</code></td>
<td>Configures the IKE SAs key lifetime in seconds</td>
<td>page 7-68</td>
</tr>
<tr>
<td><code>ikev2</code></td>
<td>Enables/disables the forced reauthentication of IKEv2 peer</td>
<td>page 7-69</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 7-70</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negates a command or sets its default</td>
<td>page 7-71</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 — AP300, 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, 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 up to 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
  - 0 <WORD> – Enter a clear text key
  - 2 <WORD> – Enter 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
company@123 rsa
rfs7000-37FABE(config-profile-default-rfs7000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
  groupid company@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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ip nat crypto
```

**Parameters**

- `ip nat crypto`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip nat crypto</code></td>
<td>Enables unique identification of APs and the hosts present in each AP's subnet</td>
</tr>
</tbody>
</table>
|                    | 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 *remotegw* and *crypto*.

**Examples**

```
rfs4000-229D58(config-profile-test)#ip nat crypto
rfs4000-229D58(config-profile-test)#show context crypto auto-ipsec-secure
remotegw ike-version ikev2 uniqueid
 ip nat crypto
rfs4000-229D58(config-profile-test)#
```
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 — AP300, 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, 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></td>
<td>• &lt;600-86400&gt; – Specify a value from 600 - 86400 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)#
### 7.1.18.2.4 ikev2

**crypto-auto-ipsec-tunnel commands**

Enables/disables the forced IKEv2 peer re-authentication.

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 reauthenticate themselves. When enabled, IKE tunnel peers have to reauthenticate each time the IKE SA is renegotiated.

Supported in the following platforms:
- Access Points — AP300, 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, 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 reauthenticate 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

Defines the IKE version used for auto IPSEC tunnel negotiation using a secure gateway

Supported in the following platforms:
- Access Points — AP300, 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, 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</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>
</tbody>
</table>

uniqueid — Optional. Enables the assigning of a unique ID to APs (using this profile) behind a router by prefixing the MAC address to the groupid

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.

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**

Negates a command or set its defaults

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [groupid|ike-lifetime|ikev2|ip]
```

**Parameters**

- `no [groupid|ike-lifetime|ikev2|ip]`

<table>
<thead>
<tr>
<th>groupid</th>
<th>Removes local/remote identity for auto IPSec IKE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ike-lifetime</td>
<td>Removes the ISAKMP associations’ lifetime period</td>
</tr>
<tr>
<td>ikev2</td>
<td>Removes the need of peer re-authenticate in case of ike rekey</td>
</tr>
<tr>
<td>ip nat crypto</td>
<td>Disables unique identification of APs behind the NAT router</td>
</tr>
</tbody>
</table>

**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 company@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
```

```
nx4500-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#no ikev2 peer reauth
```

```
nx4500-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
  crypto auto-ipsec-secure
    no ikev2 peer reauth
```

```
nx4500-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#ike-lifetime 800
```

```
nx4500-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#no ike-lifetime
```

```
nx4500-5CFA2B(config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
  crypto auto-ipsec-secure
    no ikev2 peer reauth
```

```
nx4500-5CFA2B(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 policy config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 policy
<IKEV1/IKEV2-POLICY-NAME>
```

```
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
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-ikev1-testpolicy)#
```

```
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
```

```
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.
Table 7.6 summarizes crypto IKEv1/iKEv2 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 7-74</td>
</tr>
<tr>
<td>dpd-retries</td>
<td>Sets the maximum number of attempts for sending Dead-Peer-Detection (DPD) keep alive packets (applicable only to the IKEv1 policy)</td>
<td>page 7-75</td>
</tr>
<tr>
<td>isakmp-proposal</td>
<td>Configures ISAKMP proposals</td>
<td>page 7-76</td>
</tr>
<tr>
<td>lifetime</td>
<td>Specifies how long an IKE SA is valid before it expires</td>
<td>page 7-77</td>
</tr>
<tr>
<td>mode</td>
<td>Sets the mode of the tunnels (applicable only to the IKEv1 policy)</td>
<td>page 7-78</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 7-79</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 — AP300, 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, 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 interval 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

Sets the maximum number of attempts for sending DPD keep alive packets to a peer. Once this value is exceeded, without a response, the VPN tunnel connection is declared dead. This option is available only for the IKEv1 policy.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

dpd-retries <1-100>

Parameters
- dpd-retries <1-100>

| <1-100> | Declares a peer dead after the specified number of retries. Specify a value from 1-100. |

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
```

**Parameters**


<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Specify the name of the ISAKMP proposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption</td>
<td>Configures the encryption level transmitted using the crypto isakmp command</td>
</tr>
<tr>
<td>[3des</td>
<td>aes</td>
</tr>
<tr>
<td></td>
<td>• 3des – Configures triple data encryption standard</td>
</tr>
<tr>
<td></td>
<td>• aes – Configures AES (128 bit keys)</td>
</tr>
<tr>
<td></td>
<td>• aes-192 – Configures AES (192 bit keys)</td>
</tr>
<tr>
<td></td>
<td>• aes-256 – Configures AES (256 bit keys)</td>
</tr>
<tr>
<td>group [14</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>• 14 – Configures DH group 14</td>
</tr>
<tr>
<td></td>
<td>• 2 – Configures DH group 2</td>
</tr>
<tr>
<td></td>
<td>• 5 – Configures DH group 5</td>
</tr>
<tr>
<td>hash [md5</td>
<td>sha]</td>
</tr>
<tr>
<td></td>
<td>• md5 – Uses Message Digest 5 (MD5) hash algorithm</td>
</tr>
<tr>
<td></td>
<td>• sha – Uses Secure Hash Authentication (SHA) hash algorithm</td>
</tr>
</tbody>
</table>

**Examples**

```
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-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-testpolicy)#
```
7.1.18.3.4 lifetime

- **crypto-ikev1/ikev2-policy commands**

  Specifies how long an IKE SA is valid before it expires

  Supported in the following platforms:
  - Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
lifetime <600-86400>
```

**Parameters**

- lifetime <600-86400>

<table>
<thead>
<tr>
<th>&lt;lifetime 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>-- Specify a value from 600 - 86400 seconds.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-policy-test-ikev1policy)#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 testpraposal 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

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

mode [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 testpraposal 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**

Negates a command or set its defaults

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [dpd-keepalive|dpd-retries|isakmp-proposal|lifetime|mode]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dpd-keepalive</td>
<td>Resets the DPD keepalive interval to default</td>
</tr>
<tr>
<td>dpd-retries</td>
<td>Resets the DPD keepalive retries count to default (applicable only to the IKEv1 policy)</td>
</tr>
<tr>
<td>isakmp-proposal</td>
<td>Removes the configured ISAKMP proposal</td>
</tr>
<tr>
<td>lifetime</td>
<td>Resets the ISAKMP security association lifetime</td>
</tr>
<tr>
<td>mode</td>
<td>Resets the tunnelling mode to default (main mode) (applicable only to the IKEv1 policy)</td>
</tr>
</tbody>
</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 testpraposal encryption aes group 2 hash sha
  mode aggressive
```

```
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
```

The following example shows the IKEV1 Policy settings after the 'no' commands are executed:

```
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 testpraposal 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 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)#
```

**Table 7.7 summarizes crypto IPSec IKEv1/IKEv2 peer configuration 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 credentials</td>
<td>page 7-82</td>
</tr>
<tr>
<td>ip</td>
<td>Configures the peer's IP address</td>
<td>page 7-83</td>
</tr>
<tr>
<td>localid</td>
<td>Configures a peer's local identity details</td>
<td>page 7-84</td>
</tr>
<tr>
<td>remoteid</td>
<td>Configures a remote peer's identity details</td>
<td>page 7-85</td>
</tr>
</tbody>
</table>
Table 7.7  Crypto-IKEv1/IKEv2-Peer-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>Associates a IKEv1 policy and IKEv2 policy with the IKEv1 and IKEv2 peer respectively</td>
<td>page 7-86</td>
</tr>
<tr>
<td>no</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 7-87</td>
</tr>
</tbody>
</table>
7.18.4.1 authentication

* crypto-ikev1/ikev2-peer commands

Configures IKEv1/IKEv2 peer's authentication mode and credentials

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
authentication [psk|rsa]
```

```
authentication psk [0 <WORD>|2 <WORD>|<WORD>]
```

**Parameters**

- `psk [0 <WORD>|2 <WORD>|<WORD>]`
  - Configures *pre-shared key* (PSK) authentication method
  - 0 <WORD> – Specifies a clear text key. The key must be from 8 - 21 characters
  - 2 <WORD> – Specifies an encrypted key. The key must be from 8 - 21 characters
  - <WORD> – Pre-shared key. The key must be from 8 - 21 characters

- `rsa`
  - Configures RSA-SIG authentication method

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#authentication rsa
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#authentication psk 0 test@123456
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context crypto ikev2 peer peer1
   authentication psk 0 test@123456 local
   authentication psk 0 test@123456 remote
```

```
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```
7.1.18.4.2 ip

- **crypto-ikev1/ikev2-peer commands**

Sets the IP address of the peer device. This can be set for multiple remote peers. The remote peer can be either an IP address or hostname.

Supported in the following platforms:
- Access Points — AP300, 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, 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

Sets a IKEv1/IKEv2 peer’s local identity credentials

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
localid [address|dn|email|fqdn|string]
localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]

The following command is specific to the IKEv2 peer configuration:
localid autogen-uniqueid <WORD>

Parameters
- localid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
- address <IP> Configures the peer’s IP address. The IP address is used as local identity.
- dn <WORD> Configures the peer’s distinguished name. (for example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters.
- email <WORD> Configures the peer’s e-mail address. The maximum length is 128 characters.
- fqdn <WORD> Configures the peer’s FQDN. The maximum length is 128 characters.
- string <WORD> Configures the peer’s identity string. The maximum length is 128 characters.

- localid autogen-uniqueid <WORD>
- autogen-uniqueid <WORD> Prefixes the autogen-uniqueid of the device to the string provided here. The device’s autogen-uniqueid should be existing and configured. For more information on autogen-uniqueid, see autogen-uniqueid.
- <WORD> – Provide the string that is prefixed to the device’s autogen-uniqueid.

Examples
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#localid email bob@company.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@company.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 credentials

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

remoteid [address <IP> | dn <WORD> | email <WORD> | fqdn <WORD> | string <WORD>]

**Parameters**

- **address <IP>** Configures the remote IKEv1/IKEV2 peer’s IP address. The IP address is used as the peer’s remote identity.
- **dn <WORD>** Configures the remote peer’s distinguished name. For example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters.
- **email <WORD>** Configures the remote peer’s e-mail address. The maximum length is 128 characters.
- **fqdn <WORD>** Configures a peer’s FQDN. The maximum length is 128 characters.
- **string <WORD>** Configures a peer’s identity string. The maximum length is 128 characters.

**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@company.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 configuration settings with IKEv1/IKEv2 peer

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
use ikev1-policy <IKEV1-POLICY-NAME>
use ikev2-policy <IKEV2-POLICY-NAME>
```

**Parameters**

- **use ikev1-policy <IKEV1-POLICY-NAME>**
  
  - Specify the IKEv1 policy name.
  - The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations.

- **use ikev2-policy <IKEV2-POLICY-NAME>**
  
  - Specify the IKEv2 policy name.
  - The local IKE policy and the peer IKE 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
remoteid dn SanJose
localid email bob@company.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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [authentication|ip|localid|remoteid|use]
```

**Parameters**

- no [authentication|ip|localid|remoteid|use]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no authentication</td>
<td>Removes a IKEv1/IKEv2 peer’s authentication credentials</td>
</tr>
<tr>
<td>no ip</td>
<td>Removes a IKEv1/IKEv2 peer’s IP address / FQDN</td>
</tr>
<tr>
<td>no localid</td>
<td>Removes a IKEv1/IKEv2 peer’s local identity details</td>
</tr>
<tr>
<td>no remoteid</td>
<td>Removes a IKEv1/IKEv2 peer’s remote identity details</td>
</tr>
<tr>
<td>no use</td>
<td>Removes the IKEv1/IKEv2 policy associated with IKEv1/IKEv2 peer respectively</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the Crypto IKEV1 peer1 settings before the ‘no’ commands are executed:

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
  ip address 172.16.10.12
  remotedn SanJose
  localid email bob@company.com
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

```plaintext
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 IKEV1 peer1 settings after the ‘no’ commands are executed:

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
  ip address 172.16.10.12
  use ikev1-policy test-ikev1policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev1-peer-peer1)#
```

The following example shows the Crypto IKEV2 peer1 settings before the ‘no’ commands are executed:

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
  remotedn 157.235.209.63
  use ikev2-policy
rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#
```
The following example shows the Crypto IKEV2 peer1 settings after the 'no' commands are executed:

rfs7000-37FABE(config-profile-default-rfs7000-ikev2-peer-peer1)#no use ikev2-policy
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 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).

Internet Key Exchange (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 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 | ipsec-manual]

In the profile-config mode:
<DEVICE>(config-profile-PROFILE-NAME)#crypto map <CRYPTO-MAP-TAG> <1-1000>
    [ipsec-isakmp | 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).

Manual Crypto Map Configuration commands:
local-endpoint-ip    Use this IP as local tunnel endpoint address, instead
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

rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1#)

Table 7.10 summarizes crypto map configuration mode commands.

**Table 7.8  Crypto-Map-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 7-91</td>
</tr>
<tr>
<td>crypto-map-ipsec-manual-instance</td>
<td>Configures a manual site-to-site VPN</td>
<td>page 7-105</td>
</tr>
</tbody>
</table>
7.1.18.6 crypto-map auto-vpn-tunnel/remote-vpn-client instance

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
- 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
- show: Show running system information
- write: Write running configuration to memory or terminal
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#2)#

Table 7.9 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. This command is applicable only to the site-to-site VPN tunnel.</td>
<td>page 7-93</td>
</tr>
<tr>
<td>local-endpoint-ip</td>
<td>Uses the configured IP as local tunnel endpoint address, instead of the interface IP. This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td>page 7-94</td>
</tr>
<tr>
<td>modeconfig</td>
<td>Configures the mode config method (pull or push) associated with the remote VPN client. This command is applicable only to the remote VPN client.</td>
<td>page 7-95</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the IKEv1 or IKEv2 peer for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td>page 7-96</td>
</tr>
<tr>
<td>pfs</td>
<td>Configures the Perfect Forward Secrecy (PFS) for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td>page 7-97</td>
</tr>
<tr>
<td>remote-type</td>
<td>Configures the remote VPN client type as either None or XAuth. This command is applicable only to the remote VPN client.</td>
<td>page 7-98</td>
</tr>
<tr>
<td>security-association</td>
<td>Defines this automatic VPN tunnel’s IPSec SA settings. This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td>page 7-99</td>
</tr>
<tr>
<td>transform-set</td>
<td>Applies a transform set (encryption and hash algorithms) to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td>page 7-101</td>
</tr>
<tr>
<td>use</td>
<td>Applies an existing and configured IP access list to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.</td>
<td>page 7-102</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts site-to-site VPN tunnel or remote VPN client settings</td>
<td>page 7-103</td>
</tr>
</tbody>
</table>
7.1.18.6.1 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 setting is disabled by default.

Supported in the following platforms:

- Access Points — AP300, 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, 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)#
### 7.1.18.6.2 local-endpoint-ip

Uses the configured IP as local tunnel endpoint address, instead of the interface IP

**Supported in the following platforms:**
- Access Points — AP300, 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, 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>Configures the local VPN tunnel's (site-to-site VPN tunnel or remote VPN client) endpoint IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt;</td>
<td>Specify the IP address. The specified IP address must be available on the interface.</td>
</tr>
</tbody>
</table>

**Examples**

**Site-to-site VPN tunnel:**
```
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:**
```
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)#
```
7.1.18.6.3 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 — AP300, 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, 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 push
7.1.18.6.4 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, 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></td>
<td>• <code>&lt;IKEv1-PEER-NAME&gt;</code> — Specify the IKEv1 peer’s name.</td>
</tr>
<tr>
<td>ikev2 &lt;IKEv2-PEER-NAME&gt;</td>
<td>Configures an IKEv2 peer</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IKEv2-PEER-NAME&gt;</code> — Specify the IKEv2 peer’s name.</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)#
```
### 7.1.18.6.5 pfs

**crypto-map auto-vpn-tunnel/remote-vpn-client instance**

Configures the **Perfect Forward Secrecy** (PFS) for the auto site-to-site VPN tunnel or remote VPN client. PFS is a 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. The option is disabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
pfs [14|2|5]
```

**Parameters**

- **pfs [14|2|5]**
  - Configures the PFS
    - 14 – Configures D-H Group14 (2048-bit modp)
    - 2 – Configures D-H Group2 (1024-bit modp)
    - 5 – D-H Group5 (1536-bit modp)

**Examples**

**Site-to-site VPN tunnel:**

```
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:**

```
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)#
```
7.1.18.6.6 remote-type

```
79x677  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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
remote-type [none|xauth]
```

**Parameters**

- remote-type [none|xauth]

| remote-type [none|xauth] | Specify the remote VPN’s client type |
|-------------------------|-------------------------------------|
| none                    | Specifies remote VPN client with No XAUTH |
| xauth                   | Specify remote VPN client as using XAUTH (applicable only for IKEv1). This is the default setting |

**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. The default setting is 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)#
```
**7.18.6.7 security-association**

* crypto-map auto-vpn-tunnel/remote-vpn-client instance

Defines the IPSec SAs (created by this auto site-to-site VPN tunnel or remote VPN client) settings

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
security-association [inactivity-timeout|level|lifetime]
```

```
security-association [inactivity-timeout <120-86400>|level prehost]
```

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

**Parameters**

<table>
<thead>
<tr>
<th>inactivity-timeout &lt;120-86400&gt;</th>
<th>Specifies an inactivity period, in seconds, for this IPSec VPN SA. Once the set value is exceeded, the association is timed out.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;120-86400&gt;</td>
<td>&lt;120-86400&gt; – Specify a value from 120 - 86400 seconds. The default is 900 seconds.</td>
</tr>
<tr>
<td>level prehost</td>
<td>Specifies the granularity level for this IPSec VPN SA</td>
</tr>
<tr>
<td>prehost – Sets the IPSec VPN SA's granularity to the host level</td>
<td></td>
</tr>
</tbody>
</table>

**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 prehost
```

```
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)#
### 7.18.6.8 transform-set

Applies a transform set (encryption and hash algorithms) to site-to-site VPN tunnel or remote VPN client. This command allows you 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
transform-set <TRANSFORM-SET-TAG>
```

#### Parameters

- `transform-set <TRANSFORM-SET-TAG>`

| transform-set <TRANSFORM-SET-TAG> | Applies a transform set. The transform set should be existing and configured
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TRANSFORM-SET-TAG&gt;</td>
<td>Specifying the transform set's name example: <code>transform-set AutoVPN</code></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)#
```
7.18.6.9 use

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax

use ip-access-list <IP-ACCESS-LIST-NAME>

Parameters

- use ip-access-list <IP-ACCESS-LIST-NAME>

Examples

Site-to-site VPN tunnel:

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:

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)#
7.1.18.6.10 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [ip|local-endpoint|modeconfig|peer|pfs|remote-type|security-association|
transform-set|use]
```

**Parameters**

- `no [ip|local-endpoint|modeconfig|peer|pfs|remote-type|security-association|
transform-set|use]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ip</td>
<td>Disables this setting to utilize IP/Port NAT on the auto site-to-site VPN tunnel</td>
</tr>
<tr>
<td>no local-endpoint-ip</td>
<td>Removes the configured IP as local tunnel endpoint address</td>
</tr>
<tr>
<td>no modeconfig</td>
<td>Resets the remote VPN client’s mode config method to default (push)</td>
</tr>
<tr>
<td>no peer</td>
<td>Removes the configured IKEv1 or IKEv2 peer for the auto site-to-site VPN tunnel or remote VPN client</td>
</tr>
<tr>
<td>no pfs</td>
<td>Removes the PFS configured for this auto site-to-site VPN tunnel</td>
</tr>
<tr>
<td>no remote-type</td>
<td>Resets the remote VPN client type to default (XAUTH)</td>
</tr>
<tr>
<td>no security-association</td>
<td>Removes the VPN tunnel or remote VPN client’s IPSec SA settings</td>
</tr>
<tr>
<td>no transform-set</td>
<td>Removes the transform set applied to the VPN tunnel or remote VPN client</td>
</tr>
<tr>
<td>no use</td>
<td>Removes IP access list applied to the auto site-to-site VPN tunnel or remote VPN client</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the IPSec site-to-site VPN tunnel ‘test’ settings before the 'no' commands are executed:

```plaintext
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 250000t
    security-association inactivity-timeout 200
    transform-set AutVPN
    ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

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)#

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)#
7.1.18.7 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:
- 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

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#

Table 7.10 lists the IPSec manual VPN tunnel configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-endpoint-ip</td>
<td>Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)</td>
<td>page 7-106</td>
</tr>
<tr>
<td>mode</td>
<td>Sets the tunnel mode</td>
<td>page 7-107</td>
</tr>
<tr>
<td>peer</td>
<td>Sets the peer device’s IP address</td>
<td>page 7-108</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 7-109</td>
</tr>
<tr>
<td>session-key</td>
<td>Defines encryption and authentication keys for a crypto map</td>
<td>page 7-110</td>
</tr>
<tr>
<td>use</td>
<td>Uses the configured IP access list</td>
<td>page 7-112</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 7-113</td>
</tr>
</tbody>
</table>
7.1.18.7.1 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 — AP300, 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, 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>&lt;IP&gt;</td>
<td>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
```
7.1.18.7.2 mode

Sets the crypto map tunnel mode

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

mode [transport|tunnel]

Parameters

- mode [transport|tunnel]

| mode [transport|tunnel] | Sets the mode of the tunnels 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)#
7.1.18.7.3 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 — AP300, 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, 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

```
peer 172.16.10.12
```

```
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 1 ipsec-manual

peer 172.16.10.12
```

```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1)#
```
7.1.18.7.4 security-association

Define the lifetime (in kilobytes and/or seconds) of IPSec SAs created by this crypto map.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

Parameters
```
- security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

<table>
<thead>
<tr>
<th>lifetime</th>
<th>Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association.</th>
</tr>
</thead>
<tbody>
<tr>
<td>kilobytes &lt;500-2147483646&gt;</td>
<td>- Defines volume based key duration. Specify a value from 500 - 2147483646 bytes.</td>
</tr>
<tr>
<td>seconds &lt;120-86400&gt;</td>
<td>- Defines time based key duration. Specify the time frame from 120 - 86400 seconds.</td>
</tr>
</tbody>
</table>

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
crypto map map2 2 ipsec-isakmp
security-association lifetime seconds 123
```
```
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map2#2)#
```
### 7.1.18.7.5 session-key

**crypto-map-ipsec-manual-instance**

Defines encryption and authentication keys for this crypto map.

**Supported in the following platforms:**
- Access Points — AP300, 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, 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;</td>
</tr>
<tr>
<td>session-key [inbound</td>
<td>outbound] ah &lt;256-4294967295&gt; [0</td>
</tr>
<tr>
<td>session-key [inbound</td>
<td>outbound] esp &lt;256-4294967295&gt; [0</td>
</tr>
<tr>
<td></td>
<td>Sets the SPI for the security association from 256 - 4294967295.</td>
</tr>
</tbody>
</table>

**Parameters**

- **session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator [md5|sha]] <WORD>**
- **session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher [3des|aes|aes-192|aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>**

- **ah <256-4294967295>**
  - Configures authentication header (AH) as the security protocol for the security session.
  - 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.

- **[0|2|authenticator [md5|sha] <WORD>**
  - Specifies the key type.
  - **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.

- **esp <256-4294967295>**
  - Configures Encapsulating Security Payloads (ESP) as the security protocol for the security session.
  - 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)#
```
7.1.18.7.6 use

- crypto-map-ipsec-manual-instance

Uses the configured IP access list

Supported in the following platforms:

- Access Points — AP300, 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, 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
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)#
7.1.18.7.7 no

crypto-map-ipsec-manual-instance

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [local-endpoint-ip|mode|peer|security-association|session-key|use]

Parameters

- no [local-endpoint-ip|mode|peer|security-association|session-key|use]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no local-endpoint-ip</td>
<td>Deletes the local IP address</td>
</tr>
<tr>
<td>no mode</td>
<td>Resets the tunnelling mode to default (Tunnel)</td>
</tr>
<tr>
<td>no peer</td>
<td>Deletes the remote peer settings</td>
</tr>
<tr>
<td>no security-association</td>
<td>Deletes the security association parameters</td>
</tr>
<tr>
<td>no session-key</td>
<td>Deletes the session key parameters</td>
</tr>
<tr>
<td>no use</td>
<td>Resets the IP access list parameters values</td>
</tr>
</tbody>
</table>

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)#
7.1.18.8 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 an 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`

Table 7.11 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>peer</td>
<td>Adds a remote IKEv2 peer</td>
<td>page 7-115</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables the remote VPN client</td>
<td>page 7-116</td>
</tr>
<tr>
<td>transform-set</td>
<td>Associates an existing IPSec transform set with this remote VPN client</td>
<td>page 7-117</td>
</tr>
<tr>
<td>no</td>
<td>Removes the remote VPN client settings</td>
<td>page 7-118</td>
</tr>
</tbody>
</table>
7.1.18.8.1 peer

**crypto-remote-vpn-client commands**

Adds a new remote peer. 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

**Parameters**

- `peer <1-3> ikev2 <IKEV2-PEER-NAME>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer &lt;1-3&gt;</td>
<td>Adds a IKEv2 peer. You can add multiple peers to achieve redundancy</td>
</tr>
<tr>
<td>ikev2</td>
<td>Specify a priority level for the peer from 1 - 3 (1 = primary, 2 and 3 = redundant).</td>
</tr>
<tr>
<td>&lt;IKEV2-PEER-NAME&gt;</td>
<td>Specifies a name for this IKEv2 peer.</td>
</tr>
</tbody>
</table>

**Examples**

```
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)#
```
7.1.18.2 shutdown

Disables remote-vpn-client on this profile or device. Remote VPN client feature is disabled by default.
To enable remote VPN client, use the no > shutdown command.

Supported in the following platforms:
- Access Points — AP300, 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, 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)#

crypto-remote-vpn-client commands
7.1.18.8.3 transform-set

crypto-remote-vpn-client commands

Specifies the IPSec Transform to use with the 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

Syntax
transform-set <IPSEC-XFORM-TAG>

Parameters
- transform-set <IPSEC-XFORM-TAG>

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)#
7.1.18.8.4 no

*crypto-remote-vpn-client commands*

Removes the remote VPN client settings

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

no [peer <1-3>|shutdown|transform-set]

**Parameters**

- no [peer <1-3>|shutdown|transform-set]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no peer &lt;1-3&gt;</td>
<td>Removes the remote IKEv2 peer with the specified priority</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Enables remote VPN client</td>
</tr>
<tr>
<td>transform-set</td>
<td>Disassociates the transform set attached with this remote VPN client</td>
</tr>
</tbody>
</table>

**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)#

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 device-upgrade

**Profile Config Commands**

Configures device firmware upgrade settings on this profile. Access points, wireless controllers, and service platforms using this profile automatically upgrade firmware on adopted devices.

Supported in the following platforms:
- **Access Points** — AP300, 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, 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|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000)]
device-upgrade auto {(ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|ap7502|ap7522|ap7532|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000)}
device-upgrade count <1-20>
device-upgrade persist-images
```

**Parameters**

- **device-upgrade add-auto**
  - 
  - **add-auto**

  Configures a list of devices types for automatic firmware upgrade

  This command specifies the types of devices that can be automatically upgraded (if enabled). To enable automatic device firmware upgrade, use the ‘auto’ command. When enabled, access points, wireless controllers, and service platforms, using this profile, will automatically upgrade firmware on adopted devices that match the specified device types.

  - **ap621** – Adds AP621 device to the auto device type list
  - **ap622** – Adds AP622 device to the auto device type list
  - **ap650** – Adds AP650 device to the auto device type list
  - **ap6511** – Adds AP6511 device to the auto device type list
  - **ap6521** – Adds AP6521 device to the auto device type list
  - **ap6522** – Adds AP6522 device to the auto device type list
  - **ap6532** – Adds AP6532 device to the auto device type list
  - **ap6562** – Adds AP6562 device to the auto device type list
  - **ap71xx** – Adds AP71XX device to the auto device type list
  - **ap7502** – Adds AP7502 device to the auto device type list
  - **ap7522** – Adds AP7522 device to the auto device type list
  - **ap7532** – Adds AP7532 device to the auto device type list
  - **ap81xx** – Adds AP81XX device to the auto device type list
  - **ap82xx** – Adds AP82XX device to the auto device type list
  - **rfs4000** – Adds RFS4000 device to the auto device type list
  - **rfs6000** – Adds RFS6000 device to the auto device type list
  - **rfs7000** – Adds RFS7000 device to the auto device type list
  - **nx45xx** – Adds NX45XX device to the auto device type list
  - **nx65xx** – Adds NX65XX device to the auto device type list
  - **nx75xx** – Adds NX75XX device to the auto device type list
  - **nx9000** – Adds NX9000 device to the auto device type list

<table>
<thead>
<tr>
<th><strong>device-upgrade add-auto</strong></th>
<th>Adds selected devices to the device type list</th>
</tr>
</thead>
</table>
| [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] | Adds AP621 – Adds AP621 device to the auto device type list
  - **AP622** – Adds AP622 device to the auto device type list
  - **AP650** – Adds AP650 device to the auto device type list
  - **AP6511** – Adds AP6511 device to the auto device type list
  - **AP6521** – Adds AP6521 device to the auto device type list
  - **AP6522** – Adds AP6522 device to the auto device type list
  - **AP6532** – Adds AP6532 device to the auto device type list
  - **AP6562** – Adds AP6562 device to the auto device type list
  - **AP71XX** – Adds AP71XX device to the auto device type list
  - **AP7502** – Adds AP7502 device to the auto device type list
  - **AP7522** – Adds AP7522 device to the auto device type list
  - **AP7532** – Adds AP7532 device to the auto device type list
  - **AP81XX** – Adds AP81XX device to the auto device type list
  - **AP82XX** – Adds AP82XX device to the auto device type list
  - **RFS4000** – Adds RFS4000 device to the auto device type list
  - **RFS6000** – Adds RFS6000 device to the auto device type list
  - **RFS7000** – Adds RFS7000 device to the auto device type list
  - **NX45XX** – Adds NX45XX device to the auto device type list
  - **NX65XX** – Adds NX65XX device to the auto device type list
  - **NX75XX** – Adds NX75XX device to the auto device type list
  - **NX9000** – Adds NX9000 device to the auto device type list

Contd..
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.

Selects the device types for automatic firmware upgrade

- AP621 – Optional. Enables automatic AP621 firmware image upgrade
- AP622 – Optional. Enables automatic AP622 firmware image upgrade
- AP650 – Optional. Enables automatic AP650 firmware image upgrade
- AP6511 – Optional. Enables automatic AP6511 firmware image upgrade
- AP6521 – Optional. Enables automatic AP6521 firmware image upgrade
- AP6522 – Optional. Enables automatic AP6522 firmware image upgrade
- AP6532 – Optional. Enables automatic AP6532 firmware image upgrade
- AP7502 – Optional. Enables automatic AP7502 firmware image upgrade
- AP7522 – Optional. Enables automatic AP7522 firmware image upgrade
- AP7532 – Optional. Enables automatic AP7532 firmware image upgrade
- AP71XX – Optional. Enables automatic AP71XX firmware image upgrade
- AP81XX – Optional. Enables automatic AP81XX firmware image upgrade
- AP82XX – Optional. Enables automatic AP82XX firmware image upgrade
- RFS4000 – Optional. Enables automatic RFS4000 firmware image upgrade
- RFS6000 – Optional. Enables automatic RFS6000 firmware image upgrade
- RFS7000 – Optional. Enables automatic RFS7000 firmware image upgrade
- NX45XX – Optional. Enables automatic NX45XX firmware image upgrade
- NX65XX – Optional. Enables automatic NX65XX firmware image upgrade
- NX75XX – Optional. Enables automatic NX75XX firmware image upgrade
- NX9000 – Optional. Enables automatic NX9000 firmware image upgrade

Multiple device types can be added to the auto list
### device-upgrade count <1-20>

**device-upgrade count <1-20>**

- Configures the maximum number of concurrent upgrades possible
- **<1-20>** – specify a value from 1 - 20.

### device-upgrade persist-images

**device-upgrade persist-images**

- Configures parameters for automatic firmware upgrade of adopted devices. Use this command to select the device types and the maximum number of concurrent upgrades.
- **images** Enables RF Domain manager to retain AP firmware image after upgrade, subject to availability of space
- By default this feature is enabled for wireless controllers and disabled for access points.

#### Examples

```
rfs4000-229D58(config-profile-default-rfs4000)#device-upgrade auto ap71xx
```

```
rfs4000-229D58(config-profile-default-rfs4000)#show context
```

```
profile rfs4000 default-rfs4000
  autoinstall configuration
  autoinstall firmware
  **device-upgrade auto ap71xx**
  device-upgrade persist-ap-image
  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 radio1
  interface radio2
  interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  interface gel
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  --More--
  rfs4000-229D58(config-profile-default-rfs4000)#
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes device firmware upgrade settings on this profile</td>
</tr>
<tr>
<td><strong>device-upgrade</strong></td>
<td>Displays device upgrade details</td>
</tr>
</tbody>
</table>
7.1.20 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 — ES6510, AP6511, AP71XX, AP81XX, AP7502, AP7522, AP7532,
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

dot1x [guest-vlan|holdtime|system-auth-control|use]

dot1x system-auth-control

dot1x holdtime <0-600>

dot1x guest-vlan supplicant

dot1x use aaa-policy <AAA-POLICY-NAME>

Parameters

- **system-auth-control**

  Enables or disables system auth control. Enables/disables dot1x authorization globally for the controller. This feature is disabled by default.

- **dot1x holdtime <0-600>**

  Configures a holdtime interval. This is the interval after which an authentication attempt is ignored or failed.

  - <0-600> — Specify a value from 0 - 600 seconds.

  Adding a hold time at startup allows time for the network to converge before receiving or transmitting 802.1x authentication packets.

- **dot1x guest-vlan supplicant**

  Configures guest VLAN and supplicant behavior

  This feature is disabled by default.

  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 with this access point profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;AAA-POLICY-NAME&gt; – Specify the AAA policy name. Once specified, this AAA policy is utilized for authenticating user requests.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#dot1x use aaa-policy test
```

```
rfs7000-37FABE(config-profile-default-rfs7000)#dot1x system-auth-control
```

```
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 pppoe1
    use firewall-policy default
    ap300 00-15-70-63-4F-86 adopt
    ap300 00-15-70-63-4F-97 adopt
    ap300 00-A0-F8-CF-1E-DA adopt
    service pm sys-restart
    router ospf
    dot1x system-auth-control
    dot1x use aaa-policy test
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

| no | Disables or reverts settings to their default |
### 7.1.21 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 — AP300, 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, 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.</td>
</tr>
</tbody>
</table>

#### 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 |
7.1.22 email-notification

Profile Config Commands

Configures e-mail notification settings

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

email-notification [host|recipient]

email-notification recipient <RECIPIENT-NAME>

email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {port|username}

email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {username <SMTP-USERNAME>} {password [2 <WORD>|<WORD>]}

email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {username <SMTP-USERNAME>} {password [2 <WORD>|<WORD>]} {port <1-65535>}

Parameters

- email-notification recipient <RECIPIENT-EMAIL>

<table>
<thead>
<tr>
<th>recipient &lt;RECIPIENT-EMAIL&gt;</th>
<th>Defines the recipient’s e-mail address. A maximum of 6 (six) e-mail addresses can be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;RECIPIENT-EMAIL&gt; – Specify the recipient’s e-mail address (should not exceed 64 characters in length).</td>
</tr>
</tbody>
</table>

- email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {port <1-65535>}

<table>
<thead>
<tr>
<th>host &lt;SMTP-SERVER-IP&gt;</th>
<th>Configures the host SMTP server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;SMTP-SERVER-IP&gt; – Specify the SMTP server’s IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>sender &lt;SENDER-EMAIL&gt;</th>
<th>Defines the sender’s e-mail address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;SENDER-EMAIL&gt; – Specify the sender’s e-mail address (should not exceed 64 characters in length).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port &lt;1-65535&gt;</th>
<th>Optional. Configures the SMTP server port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Specify the port from 1 - 65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>username &lt;SMTP-USERNAME&gt;</th>
<th>Optional. Configures the SMTP username</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;SMTP-USERNAME&gt; – Specify the SMTP username (should not exceed 64 characters in length).</td>
</tr>
</tbody>
</table>

| password [2 <WORD>|<WORD>] | Configures the SMTP server password |
|-----------------------------|-----------------------------------|
|                            | • 2 <WORD> – Configures an encrypted password |
|                            | • <WORD> – Specify the password (should not exceed 127 characters in length). |
- `email-notification host <SMTP-SERVER-IP> sender <SENDER-EMAIL> {username <SMTP-USERNAME>} [password [2 <WORD>|<WORD>] {port <1-65535}>}

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Configures the host SMTP server</td>
</tr>
<tr>
<td>&lt;SMTP-SERVER-IP&gt;</td>
<td>- <code>&lt;SMTP-SERVER-IP&gt;</code> – Specify the IP address of the SMTP server.</td>
</tr>
<tr>
<td>sender</td>
<td>Defines sender’s e-mail address</td>
</tr>
<tr>
<td>&lt;SENDER-EMAIL&gt;</td>
<td>- <code>&lt;SENDER-EMAIL&gt;</code> – Specify sender’s e-mail address.</td>
</tr>
<tr>
<td>username</td>
<td>Optional. Configures the SMTP username</td>
</tr>
<tr>
<td>&lt;SMTP-USERNAME&gt;</td>
<td>- <code>&lt;SMTP-USERNAME&gt;</code> – Specify the SMTP username.</td>
</tr>
<tr>
<td>password</td>
<td>Configures the SMTP server password</td>
</tr>
<tr>
<td>[2 &lt;WORD&gt;</td>
<td>&lt;WORD&gt;]</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;WORD&gt;</code> – Specify the password.</td>
</tr>
<tr>
<td>port</td>
<td>Optional. Configures the SMTP server port</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>- <code>&lt;1-65535&gt;</code> – Specify the port from 1 - 65535.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000)#email-notification recipient test@company.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
go trust dscp
go trust 802.1p
use firewall-policy default
email-notification recipient test@company.com
service pm sys-restart
rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

- `no` Disables or reverts settings to their default
### 7.1.23 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** — AP300, 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, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adoption</td>
<td>Verifies firmware versions before adopting</td>
</tr>
<tr>
<td>cluster</td>
<td>Verifies firmware versions before clustering</td>
</tr>
<tr>
<td>full</td>
<td>Allows adoption or clustering when the first four octets of the firmware versions match (for example 5.4.2.0)</td>
</tr>
<tr>
<td>major</td>
<td>Allows adoption or clustering when the first two octets of the firmware versions match (for example 5.4)</td>
</tr>
<tr>
<td>minor</td>
<td>Allows adoption or clustering when the first three octets of the firmware versions match (for example 5.4.2)</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 5.4.2.0-006D)</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#enforce-version cluster full
rfs7000-37FABE(config-profile-default-rfs7000)#enforce-version adoption major
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
    bridging-mode isolated-tunnel

interface pppoe1
  use firewall-policy default
  ap300 00-15-70-63-4F-86 adopt
  ap300 00-15-70-63-4F-97 adopt
  ap300 00-A0-F8-CF-1E-DA adopt
  enforce-version adoption major
  enforce-version cluster full
  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 or reverts settings to their default</td>
</tr>
</tbody>
</table>
7.1.24 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]

evironmental-sensor [humidity|motion|polling-interval <1-100>|temperature]

evironmental-sensor light {holdtime|radio-shutdown|threshold}

evironmental-sensor light {holdtime <2-201>|radio-shutdown [all|radio-1|radio-2]}

evironmental-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      | 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 11 seconds. |
| temperature           | Enables (turns on) temperature sensors. This setting is enabled by default. |

- environmental-sensor light {holdtime <2-201>|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 <2-201>      | Optional. Configures a holdtime, in seconds, for the light sensor  
  - <2-201> – Specify a value from 2 - 201 seconds. |
| radio-shutdown [all|radio1|radio2] | Optional. Shuts down the sensor's radios  
  - all – Shuts down all radios  
  - radio1 – Shuts down radio 1  
  - radio2 – Shuts down radio 2 |

**Note:** AP8132’s using this profile have their radios shut down, when the radio’s power falls below the specified threshold.
- `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 lumens. This value determines whether lighting is on in the AP8132's deployment location. The default is 500 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 lumens. This value determines whether lighting is off in the AP8132's deployment location. The default is 100 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
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--
rfs4000-229D58 (config-profile-testRFS4000)#
```

**Related Commands**

- `no` | Removes the environmental sensor's settings |
7.1.25 events

Profile Config Commands

Displays system event messages

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
events [forward on|on]
```

Parameters

- event [forward on|on]

<table>
<thead>
<tr>
<th>forward</th>
<th>on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwards system event messages to the wireless controller, service platform, or cluster members. This feature is enabled by default.</td>
<td>Generates system events. This feature is enabled by default.</td>
</tr>
<tr>
<td>- on – Enables forwarding of system events</td>
<td></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
7.1.26 export

Profile Config Commands

Enables export of startup.log file after every boot

Supported in the following platforms:

- Access Points — AP300, 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, 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

- **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 - 86400 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>[:port]/path/file

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#export startup-log max-retries 10
retry-interval 30 url test@company.com

rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  ......................................................
  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
export startup-log max-retries 10 retry-interval 30 url test@company.com

rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

**no** — Disables export of startup.log file
7.1.27 floor

Profile Config Commands

Sets the floor name where the system is located

Supported in the following platforms:
- Access Points — AP300, 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, 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 system is located</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Specify the floor name.</td>
</tr>
</tbody>
</table>
|                          | • <1-4094> – Optional. Configures the floor number from 1 - 4094.

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
### 7.1.28 gre

*Profile Config Commands*

<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 7-134</td>
</tr>
<tr>
<td>gre-config-instance</td>
<td>Summarizes GRE tunnel configuration mode commands</td>
<td>page 7-136</td>
</tr>
</tbody>
</table>
7.1.28.1 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.

**NOTE:** Only one GRE tunnel can be created for every profile.

Supported in the following platforms:

- **Access Points** — AP300, 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, 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>&lt;GRE-TUNNEL-NAME&gt;</td>
<td>— If creating a new tunnel, specify a unique name for it. If modifying an existing tunnel, specify its name.</td>
</tr>
</tbody>
</table>

**Examples**

```Shell
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#?
```

**GRE Tunnel Mode commands**:

- `dscp` Differentiated Services Code Point
- `failover` Gre tunnel failover
- `native` Native trunking characteristics
- `no` Negate a command or set its defaults
- `peer` GRE peer
- `tunneled-vlan` VLANs to tunnel
- `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

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 |
### 7.1.28.2 gre-config-instance

The `gre` command allows you to configure GRE tunnel settings. Table 7.13 summarizes GRE tunnel configuration mode commands.

#### Table 7.13 GRE-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dscp</code></td>
<td>Sets the GRE tunnel’s Differentiated Services Code Point (DSCP) / 802.1q priority value</td>
<td>page 7-137</td>
</tr>
<tr>
<td><code>failover</code></td>
<td>Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable</td>
<td>page 7-138</td>
</tr>
<tr>
<td><code>native</code></td>
<td>Configures native trunking settings for this GRE tunnel</td>
<td>page 7-139</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Removes the GRE tunnel settings based on the parameters passed</td>
<td>page 7-140</td>
</tr>
<tr>
<td><code>peer</code></td>
<td>Configures the GRE tunnel’s end-point peers</td>
<td>page 7-142</td>
</tr>
<tr>
<td><code>tunneled-vlan</code></td>
<td>Defines the VLAN that connected clients use to route GRE-tunneled traffic within their respective WLANs</td>
<td>page 7-143</td>
</tr>
</tbody>
</table>
7.1.28.2.1 dscp

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 — AP300, 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, 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
7.1.28.2.2 failover

**gre-config-instance**

Enables periodic pinging of the primary gateway to assess its availability. When enabled, the system continues pinging, an unreachable gateway, for a specified number of times and at the specified interval.

This option is disabled by default.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
failover interval <0-86400> retry <0-10>
```

**Parameters**

- **failover interval <0-86400> retry <0-10>**

  - **failover interval <0-86400>**
    - Specifies the interval, in seconds, between two successive pings to the primary gateway. If the primary gateway is unreachable, the system pings it at intervals specified here.
    - `<0-86400>` – Specify a value from 0 - 86400 seconds.
  - **retry <0-10>**
    - Specifies the maximum number attempts made to ping the primary gateway before the session is terminated.
    - `<0-10>` – Specify a value from 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
### 7.1.28.2.3 native

**gre-config-instance**

Configures native trunking settings for this GRE tunnel

**Supported in the following platforms:**

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
native [tagged|vlan <1-4094>]
```

**Parameters**

- native [tagged|vlan <1-4094>]

<table>
<thead>
<tr>
<th>native tagged</th>
<th>Tags the native VLAN</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**

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#native tagged
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#native vlan 1
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context
gre tunnel testGRETunnel
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
7.1.28.2.4 no

- gre-config-instance

Removes the GRE tunnel settings based on the parameters passed

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [dscp|failover|native|peer|tunneled-vlan]

Parameters

- no [dscp|failover|native|peer|tunneled-vlan]

Examples

The following example shows the GRE tunnel ‘testGRETunnel’ settings before the no commands are executed:

```
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)#
```

```
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:

```
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
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp</td>
<td>Sets the GRE tunnel’s DSCP / 802.1q priority value</td>
</tr>
<tr>
<td>failover</td>
<td>Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable</td>
</tr>
<tr>
<td>native</td>
<td>Configures native trunking settings for this GRE tunnel</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the GRE tunnel’s end-point peers</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>
</tr>
</tbody>
</table>
### 7.1.28.2.5 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

peer <1-2> ip <IP>

**Parameters**

- peer <1-2> ip <IP>

  **Parameters**
  - peer <1-2> ip <IP>  
    - <1-2> – Specify a numeric index for each peer to help differentiate the tunnel end points.
    - ip – Specifies the IP address of the added GRE peer to serve as a network address identifier.
    - <IP> – Specify the peer’s IP address.

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the GRE tunnel settings based on the parameters passed</td>
</tr>
</tbody>
</table>
### 7.1.28.2.6 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
tunneled-vlan <VLAN-ID>
```

**Parameters**

- `tunneled-vlan <VLAN-ID>`

**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.
### 7.1.29 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 the WiNG 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. 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 hierarchically network, see device-upgrade.

Supported in the following platforms:
- **Access Points** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>http-analyze</strong></td>
<td>Configures HTTP analysis parameters. These parameters are: compress and update-interval.</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>update-interval</strong></td>
<td>Sets the interval, in seconds, at which buffered packets are pushed to analyze the HTTP connection.</td>
</tr>
<tr>
<td><strong>&lt;1-3600&gt;</strong></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

- **no** Disables HTTP analyze settings
7.1.30 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 the WiNG 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, NX6500, NX6524, NX7500, 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|user-name|
 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>http-analyze</td>
<td>Configures HTTP analysis related parameters</td>
</tr>
<tr>
<td>compress</td>
<td>Compresses update files before forwarding to the controller. This option is disabled by default.</td>
</tr>
<tr>
<td>controller</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>update-interval &lt;1-3600&gt;</td>
<td>Configures the interval, in seconds, at which buffered packets are pushed to the controller</td>
</tr>
<tr>
<td></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>http-analyze external-server</td>
<td>Configures the external HTTP analytics engine's parameters</td>
</tr>
<tr>
<td>password &lt;WORD&gt;</td>
<td>Configures the external analytics engine's password</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; -- Provide the login password.</td>
</tr>
<tr>
<td>proxy &lt;URL&gt;</td>
<td>Configures the proxy server's URL</td>
</tr>
<tr>
<td></td>
<td>• &lt;URL&gt; -- Specify the proxy server's URL in the following format: <a href="http://username:password@proxy-server:port">http://username:password@proxy-server:port</a>. For example, <a href="http://mot:80@wwwgate0.mot.com:1080">http://mot:80@wwwgate0.mot.com:1080</a></td>
</tr>
<tr>
<td>update-interval &lt;1-3600&gt;</td>
<td>Configures the interval, in seconds, at which buffered packets are pushed to the external analytics engine</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-3600&gt; – Specify the interval from 1 - 3600 seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>url &lt;URL&gt;</td>
<td>Configures the external analytics engine's IP address or uniform resource locator (URL)</td>
</tr>
<tr>
<td></td>
<td>• &lt;URL&gt; -- Provide the IP address or URL.</td>
</tr>
<tr>
<td>username &lt;WORD&gt;</td>
<td>Configures the user name needed to access the external analytics engine</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; -- Provide the user name.</td>
</tr>
<tr>
<td>validate-server-certificate</td>
<td>Validates the external analytics engine's certificate, if it is using HTTPS as the mode of access</td>
</tr>
</tbody>
</table>

### Examples

```bash
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
nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#show context
```

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

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B)#http-analyze external-server proxy
http://mot:sym@wwwgate0.mot.com:1080

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
slot 1
  no shutdown
  assign team-centro
  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 proxy http://mot:sym@wwwgate0.mot.com:1080
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><strong>no</strong></td>
<td>Disables HTTP analytics settings on an NX series service platform</td>
</tr>
</tbody>
</table>
7.1.31 interface

Profile Config Commands

Table 7.14 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 7-149</td>
</tr>
<tr>
<td>interface-config-instance</td>
<td>Summarizes Ethernet interface (associated with the wireless controller or service platform) configuration commands</td>
<td>page 7-152</td>
</tr>
<tr>
<td>interface-config-vlan-instance</td>
<td>Summarizes VLAN interface configuration commands</td>
<td>page 7-174</td>
</tr>
<tr>
<td>interface-config-radio-instance</td>
<td>Summarizes radio interface configuration commands (applicable to devices with built-in radios)</td>
<td>page 7-187</td>
</tr>
<tr>
<td>interface-config-wwan-instance</td>
<td>Summarizes WWAN interface configuration commands</td>
<td>page 7-253</td>
</tr>
<tr>
<td>interface-config-serial-instance</td>
<td>Summarizes serial interface configuration commands (supported only on the NX45XX and NX65XX series service platform profiles)</td>
<td>page 7-264</td>
</tr>
<tr>
<td>interface-config-t1e1-instance</td>
<td>Summarizes the T1E1 interface configuration commands (supported only on the NX45XX and NX65XX series service platform profiles)</td>
<td>page 7-278</td>
</tr>
<tr>
<td>interface-config-vm-instance</td>
<td>Summarizes the virtual machine interface configuration commands (supported only on the NX45XX and NX65XX series service platform profiles)</td>
<td>page 7-292</td>
</tr>
</tbody>
</table>
### 7.1.31.1 interface

Selects an interface to configure

This command is used to enter the interface configuration mode for the specified physical SVI interface. If the VLAN (SVI) interface does not exist, it is automatically created.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax Service Platforms**

```
interface [INTERFACE-NAME]|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoel|
radio [1|2|3]|serial <1-4>|t1e1 <1-4>|up <1-2>|vlan <1-4094>|vmif <1-8>|wwan1|xge <1-4>
```

**Syntax Access Points and Wireless Controllers**

```
interface [INTERFACE-NAME]|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|pppoel|
radio [1|2|3]|up1|vlan <1-4094>|wwan1|xge <1-4>
```

**Parameters**

- `interface [INTERFACE-NAME]|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|pppoel|
  - `<1-4>` — Specify the interface index from 1 - 4. 
  - This interface is applicable only for AP6511

- `ge <1-8>` — Selects a GigabitEthernet interface
  - `<1-8>` — Specify the interface index from 1 - 8. (4 for RFS7000 and 8 for RFS6000).
  - The NX45XX and NX65XX series service platforms have 24 GigabitEthernet interface ports.

- `me1` — Selects a management interface
  - Not applicable for RFS4000
  - The management interface is applicable only for RFS6000 and RFS7000

- `port-channel <1-4>` — Selects the port channel interface
  - `<1-4>` — Specify the interface index from 1 - 4.

- `pppoel` — Selects the PPP over Ethernet interface to configure

- `radio [1|2|3]` — Selects a radio interface
  - 1 — Selects radio interface 1
  - 2 — Selects radio interface 2
  - 3 — Selects radio interface 3
  - The radio interface is not available on wireless controllers (exception RFS4011) or service platforms.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| serial <1-4> | Selects a serial interface  
• <1-4> – Specify the interface index from 1 - 4.  
The serial interfaces are virtual interfaces available only on the NX45XX and NX65XX series service platforms. |
| t1e1 <1-4> | Selects the T1 and E1 slot interfaces  
• <1-4> – Specify the T1 or E1 slot ID from 1 - 4.  
The T1E1 interfaces are available only on the NX45XX and NX65XX series service platforms. |
| up1       | Selects the uplink GigabitEthernet interface  
The NX45XX and NX65XX series profiles support 2 uplink interfaces (up <1-2>) |
| vlan <1-4094> | Selects a VLAN interface  
• <1-4094> – Specify the SVI VLAN ID from 1 - 4094. |
| vmif <1-8> | Selects the virtual machine (VM) interface  
• <1-8> – Specify the VM interface index from 1 - 8.  
The VM interfaces are available only on the NX45XX, NX65XX, NX9XXX series service platforms. |
| wwan1     | Selects a Wireless WAN interface  
This interface is applicable only to AP71XX, AP81XX, AP82XX, RFS4000, RFS6000 |
| xge <1-4> | Selects a TenGigabitEthernet interface  
• <1-2> – Specify the interface index from 1 - 4. |

**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

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
- NX6500 - up1, up2
- NX6524 - ge1- ge24, up1, up2
- NX9000 series - ge1, ge2
- NX9600 - ge1- ge2, 4 usb ports

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.

**Examples**

```bash
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-relay-incoming`: Allow on-board DHCP server to respond to relayed DHCP packets on this interface
- `ip`: Interface Internet Protocol config commands
- `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

```bash
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
```

```bash
nx4500-5CFA2B(config-profile-testNX45XX)#interface vmif 2
nx4500-5CFA2B(config-profile-testNX45XX-if-vmif12)#
```

**VM Interface Mode commands:**

- `description`: Port description
- `ip`: Internet Protocol (IP)
- `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

```bash
nx4500-5CFA2B(config-profile-testNX45XX-if-vmif2)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the selected interface</td>
</tr>
</tbody>
</table>
7.1.31.2 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 <1-8>|me1|port-channel <1-4>|pppoel|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)#?

Interface configuration commands:
cdp Cisco Discovery Protocol
description Interface specific description
dot1x 802.1X
duplex Set duplex to interface
ip Internet Protocol (IP)
lldp Link Local Discovery Protocol
mac-auth Enable mac-auth for this port
no Negate a command or set its defaults
power PoE Command
qos Quality of service
shutdown Shutdown the selected interface
spanning-tree Spanning tree commands
speed Configure speed
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

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

NOTE: The NX45XX and NX65XX series service platforms have 24 GigabitEthernet ports.

Table 7.15 summarizes the interface configuration commands.

Table 7.15 Interface-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp</td>
<td>Enables Cisco Discovery Protocol (CDP) on GE ports</td>
<td>page 7-154</td>
</tr>
<tr>
<td>channel-group</td>
<td>Configures channel group commands</td>
<td>page 7-155</td>
</tr>
<tr>
<td>description</td>
<td>Creates an interface specific description</td>
<td>page 7-156</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>dot1x</strong> (authenticator)</td>
<td>Configures 802.1X authenticator settings</td>
<td>page 7-157</td>
</tr>
<tr>
<td><strong>dot1x</strong> (supplicant)</td>
<td>Configures 802.1X supplicant settings</td>
<td>page 7-159</td>
</tr>
<tr>
<td><strong>duplex</strong></td>
<td>Specifies the duplex mode for the interface</td>
<td>page 7-160</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Sets the IP address for the assigned Fast Ethernet interface (ME) and VLAN interface</td>
<td>page 7-161</td>
</tr>
<tr>
<td><strong>lldp</strong></td>
<td>Configures Link Local Discovery Protocol (LLDP)</td>
<td>page 7-162</td>
</tr>
<tr>
<td><strong>mac-auth</strong></td>
<td>Enables MAC-based port authentication on this profile</td>
<td>page 7-163</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Negates a command or sets its defaults</td>
<td>page 7-164</td>
</tr>
<tr>
<td><strong>power</strong></td>
<td>Configures Power over Ethernet (PoE) settings on this interface</td>
<td>page 7-165</td>
</tr>
<tr>
<td><strong>qos</strong></td>
<td>Enables QoS</td>
<td>page 7-166</td>
</tr>
<tr>
<td><strong>shutdown</strong></td>
<td>Disables the selected interface</td>
<td>page 7-167</td>
</tr>
<tr>
<td><strong>spanning-tree</strong></td>
<td>Configures spanning tree parameters</td>
<td>page 7-168</td>
</tr>
<tr>
<td><strong>speed</strong></td>
<td>Specifies the speed of a FastEthernet or GigabitEthernet port</td>
<td>page 7-170</td>
</tr>
<tr>
<td><strong>switchport</strong></td>
<td>Sets interface switching mode characteristics</td>
<td>page 7-171</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>Defines the settings to use with this command</td>
<td>page 7-173</td>
</tr>
</tbody>
</table>
7.1.31.2.1 cdp

Enables CDP on the selected GE port

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

cdp [receive|transmit]

Parameters

- cdp [receive|transmit]

| transmit | Enables CDP packet snooping on an interface |
| receive  | Enables CDP packet transmission on an interface |

Examples

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#cdp transmit

Related Commands

- no Disables CDP on the controller or service platform's selected GE ports
7.1.31.2.2 channel-group

```
• interface-config-instance
```

Configures a channel group

**NOTE:** Channel group is not supported on the NX45XX and NX65XX series service platforms.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000, NX9500, NX9510, NX9600

**Syntax**

```
channel-group <1-4>
```

**Parameters**

- channel-group <1-4>

<table>
<thead>
<tr>
<th>&lt;1-4&gt;</th>
<th>Specifies a channel group number from 1 - 4</th>
</tr>
</thead>
</table>

**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 a channel group |
7.1.31.2.3 description

`interface-config-instance`

Configures a description for a defined interface

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

description [\<LINE>|\<WORD>]  

**Parameters**

- description [\<LINE>|\<WORD>]

  | \<LINE> | Configures the maximum length (number of characters) of the interface description |
  | \<WORD> | Configures a unique description for this interface. The description should not exceed the length specified by the \<LINE> parameter |

**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 interface ge1
  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**

- `no`  
  Removes the interface description
7.1.31.2.4 dot1x (authenticator)

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX,
- Wireless Controllers — RFS4000, RFS6000, RFS7000

Syntax

```
dot1x authenticator [guest-vlan|host-mode|max-reauth-req|port-control|reauthenticate|timeout]
```

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]]

```
<table>
<thead>
<tr>
<th>dot1x authenticator</th>
<th>Configures 802.1x authenticator settings</th>
</tr>
</thead>
<tbody>
<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 [multi-host|single-host] | Configures the host mode for this interface
  - multi-host – Configures multiple host mode
  - single-host – Configures single host mode. This is the default setting. |
| max-reauth-req <1-10> | Configures maximum number of reauthorization retries for the supplicant. This is the maximum number of reauthentication attempts made before this port is moved to unauthorized.
  - <1-10> – Specify a value from 1 -10. The default is 2. |
```

NOTE: The dot1x (802.1x) supplicant settings are documented in the next section.
### Examples

```plaintext
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
gos trust dscp
gos 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><code>no</code></td>
<td>Disables or reverts interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.31.2.5 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, AP81XX
- 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Sets the username for authentication</td>
</tr>
<tr>
<td><code>&lt;USERNAME&gt;</code></td>
<td>Specify the username of the supplicant.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Sets the password associated with the supplicant's username.</td>
</tr>
<tr>
<td><code>[0 &lt;WORD&gt;]</code></td>
<td>Sets a clear text password</td>
</tr>
<tr>
<td><code>[2 &lt;WORD&gt;]</code></td>
<td>Sets an encrypted password</td>
</tr>
<tr>
<td><code>&lt;WORD&gt;</code></td>
<td>Specify the password.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x supplicant username bob password 0 company@123
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
interface ge1
dot1x supplicant username bob password 0 company@123
dot1x authenticator host-mode multi-host
dot1x authenticator guest-vlan 2
dot1x authenticator reauthenticate
dot1x authenticator max-reauth-count 6
ip dhcp trust
gos trust dscp
gos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

**Related Commands**

- `no` Removes 802.1X supplicant (client) settings
7.1.31.2.6 duplex

Configure duplex mode (for the flow of packets) for an interface

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
```
duplex [auto|half|full]
```

Parameters
```
- duplex [auto|half|full]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enables automatic duplexity on an interface port. The port automatically detects whether it should run in full or half-duplex mode. (default setting)</td>
</tr>
<tr>
<td>half</td>
<td>Sets the port to half-duplex mode. Allows communication in one direction only at any given time</td>
</tr>
<tr>
<td>full</td>
<td>Sets the port to full-duplex mode. Allows communication in both directions simultaneously</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
dotix supplicant username Bob password 0 company@123
ip dhcp trust
qos trust dscp
dotix supplicant username Bob password 0 company@123
ip dhcp trust
qos trust dscp
dotix supplicant username Bob password 0 company@123
ip dhcp trust
qos trust dscp
dotix supplicant username Bob password 0 company@123
dotix supplicant username Bob password 0 company@123
qos trust dscp
qos trust 802.1p
channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands
```
no
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reverts to default (auto)</td>
</tr>
</tbody>
</table>
### 7.1.31.2.7 ip

**interface-config-instance**

Sets the ARP and DHCP components for this interface

Supported in the following platforms:
- **Access Points** — AP300, 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, 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]**

| arp [header-mismatch-validation|trust] | Sets ARP for packets on this interface |
|--------------------------------------|----------------------------------------|
|                                      | • header-mismatch-validation — Verifies mismatch for source MAC address in the ARP header and Ethernet header |
|                                      | • trust — Sets the ARP trust state for ARP responses on this interface |

<table>
<thead>
<tr>
<th>dhcp trust</th>
<th>Uses a DHCP client to obtain an IP address for the interface (this enables DHCP on a layer 3 SVI)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• trust — Sets the DHCP trust state for DHXP responses on this interface</td>
</tr>
</tbody>
</table>

**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
dot1x supplicant username Bob password 0 company@123
ip dhcp trust
ip arp header-mismatch-validation
gos trust dscp
gos 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 |
7.1.31.2.8 lldp

- **interface-config-instance**

Configures *Link Local Discovery Protocol* (LLDP) parameters on the selected interface.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
lldp [receive|transmit]
```

**Parameters**

- `lldp [receive|transmit]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[receive]</td>
<td>Enables LLDP <em>Protocol Data Units</em> (PDUs) snooping</td>
</tr>
<tr>
<td>transmit</td>
<td>Enables LLDP PDUs transmission</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#lldp transmit
```

**Related Commands**

- `no` Disables or reverts interface settings to their default
7.1.31.2.9 mac-auth

- interface-config-instance

Enables authentication of MAC addresses on the selected wired port. Devices using this profile will be able to authenticate the MAC addresses of devices connecting to this GE interface.

When enabled, this feature authenticates the source MAC address of a device, connecting to this interface, with a RADIUS server. For more information on enabling this feature see, mac-auth.

To enable MAC address authentication on a device, execute the mac-auth command on the device configuration mode.

Supported in the following platforms:
- Wireless Controllers — RFS4000, RFS6000, RFS7000

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
7.1.31.2.10 no

interface-config-instance

Negates a command or sets its defaults

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
no [cdp|channel-group|description|dot1x|duplex|ip|lldp|mac-auth|power|qos|shutdown|spanning-tree|speed|switchport|use]

Parameters
None

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-if-ge1)#no cdp
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no duplex

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp</td>
<td>Enables CDP on ports</td>
</tr>
<tr>
<td>channel-group</td>
<td>Configures channel group commands</td>
</tr>
<tr>
<td>description</td>
<td>Creates an interface specific description</td>
</tr>
<tr>
<td>dot1x (authenticator)</td>
<td>Configures 802.1X authentication settings</td>
</tr>
<tr>
<td>dot1x (supplicant)</td>
<td>Configures 802.1X supplicant (client) settings</td>
</tr>
<tr>
<td>duplex</td>
<td>Specifies the duplex mode for the interface</td>
</tr>
<tr>
<td>ip</td>
<td>Sets the IP address for the assigned Fast Ethernet interface (ME) and VLAN interface</td>
</tr>
<tr>
<td>lldp</td>
<td>Configures LLDP</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables MAC-based port authentication on this profile</td>
</tr>
<tr>
<td>power</td>
<td>Configures PoE settings on this interface</td>
</tr>
<tr>
<td>qos</td>
<td>Enables QoS on the selected interface</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables the selected interface</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Configures spanning tree parameters</td>
</tr>
<tr>
<td>speed</td>
<td>Specifies the speed of a FastEthernet or GigabitEthernet port</td>
</tr>
<tr>
<td>switchport</td>
<td>Sets the interface switching mode characteristics</td>
</tr>
<tr>
<td>use</td>
<td>Defines the settings to use with this command</td>
</tr>
</tbody>
</table>
### 7.1.31.2.11 power

- **interface-config-instance**

  Configures PoE settings on this interface

**Supported in the following platforms:**
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
power {limit <0-40>|priority [critical|high|low]}
```

**Parameters**

- **power {limit <0-40>|priority [critical|high|low]}**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limit &lt;0-40&gt;</td>
<td>Optional. Configures the PoE power limit from 0 - 40 Watts</td>
</tr>
<tr>
<td>priority [critical</td>
<td>high</td>
</tr>
</tbody>
</table>

- **critical** — Sets PoE priority as critical
- **high** — Sets PoE priority as high
- **low** — Sets PoE priority as low

**Examples**

```plaintext
rfs4000-229D58 (config-profile-testRFS4000-if-gel)#power limit 30
rfs4000-229D58 (config-profile-testRFS4000-if-gel)#power priority critical
rfs4000-229D58 (config-profile-testRFS4000-if-gel)#show context
interface ge1
ip dhcp trust
gos trust dscp
gos trust 802.1p
power limit 30
power priority critical
rfs4000-229D58 (config-profile-testRFS4000-if-gel)#
```

**Related Commands**

- **no** Removes PoE settings on this interface
7.1.31.2.12 qos

- interface-config-instance

Defines Quality of Service (QoS) settings on this interface

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
qos trust [802.1p|cos|dscp]

Parameters
- qos trust [802.1p|cos|dscp]

| trust [802.1p|cos|dscp] | Trusts QoS values ingressing on this interface |
|-------------------------|-----------------------------------------------|
| 802.1p                  | 802.1p – Trusts 802.1p COS values ingressing on this interface |
| cos                     | cos – Trusts 802.1p COS values ingressing on this interface |
| dscp                    | dscp – Trusts IP DSCP QOS values ingressing on this interface |

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 a GigabitEthernet interface for Royal King
duplex full
dot1x supplicant username Bob password 0 company@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
7.1.31.2.13 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
shutdown
```

**Parameters**

None

**Examples**

```
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><code>no</code></td>
<td>Disables or reverts interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.31.2.14 spanning-tree

- interface-config-instance

Configures spanning tree parameters

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

spanning-tree [bpdufilter|bpduguard|edgeport|force-version|guard|link-type|mst|port-cisco-interoperability|portfast]

spanning-tree [edgeport|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
- spanning-tree [edgeport|force-version|guard root|portfast]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeport</td>
<td>Enables an interface as an edge port</td>
</tr>
<tr>
<td>force-version &lt;0-3&gt;</td>
<td>Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select one of the following versions:</td>
</tr>
<tr>
<td>guard root</td>
<td>Enables Root Guard for the port</td>
</tr>
<tr>
<td>portfast</td>
<td>Enables rapid transitions. Enabling PortFast allows the port to bypass the listening and learning states</td>
</tr>
</tbody>
</table>

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 BPDU from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDU.
### bpduguard

<table>
<thead>
<tr>
<th>default</th>
<th>disable</th>
<th>enable</th>
</tr>
</thead>
</table>

Enables or disables 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]

- Enables or disables point-to-point or shared link types
  - point-to-point – Enables rapid transition
  - shared – Disables rapid transition

### spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]

- Configures MST on a spanning tree
- Defines path cost for a port from 1 - 200000000
- Defines port priority for a bridge from 1 - 240

### spanning-tree port-cisco-interoperability [disable|enable]

- Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP)
- Enables CISCO Interoperability
- Disables CISCO Interoperability. The default is disabled.

### Examples

```bash
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
```

### Related Commands

- **no** Removes spanning tree settings configured on this interface
7.1.31.2.15 speed

```plaintext
 Specifications the speed of a FastEthernet (10/100) or GigabitEthernet (10/100/1000) port.

Supported in the following platforms:
- Access Points — AP300, 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, 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. Auto negotiation is a requirement for using 1000BASE-T[3] according to the standard (default setting).</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**

```plaintext
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 company@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)
### 7.1.31.2.16 switchport

**interface-config-instance**

Sets switching mode characteristics for the selected interface

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
switchport [access|mode|trunk]
switchport access vlan <1-4094>
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>]
```

#### Parameters

- **switchport access vlan <1-4094>**
  - **Sets the VLAN when interface is in the access mode**
  - `<1-4094>` – Specify the SVI VLAN ID from 1 - 4094.

- **switchport mode [access|trunk]**
  - **Sets the interface 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>]**
  - **Sets allowed VLAN options. The options are:**
  - `<VLAN-ID>` – 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.)
  - `none` – Allows no VLANs to transmit or receive through the layer 2 interface
  - `add <VLAN-ID>` – Adds VLANs to the current list
  - `<VLAN-ID>` – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.)
  - `remove <VLAN-ID>` – Removes VLANs from the current list
  - `<VLAN-ID>` – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.)
### switchport trunk native [tagged|vlan <1-4094>]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trunk</td>
<td>Sets trunking mode characteristics of the switchport</td>
</tr>
<tr>
<td>native</td>
<td>Configures the native VLAN ID for the trunk-mode port</td>
</tr>
<tr>
<td>[tagged]</td>
<td>- Tags the native VLAN</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>- Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode. Specify a value from 1 - 4094.</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

```
switchport trunk native tagged
```
```
switchport access vlan 1
```
```
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 company@123
  ip dhcp trust
  ip arp header-mismatch-validation
  qos trust dscp
  qos trust 802.1p
  channel-group 1
```

### 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>
7.1.31.2.17 use

- interface-config-instance

Specifications the IP access list and MAC access list used with this interface

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
use [ip-access-list in <IP-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]
```

Parameters

- use [ip-access-list in <IP-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>Uses an IP access list</td>
</tr>
<tr>
<td>&lt;IP-ACCESS-LIST-NAME&gt;</td>
<td>in — Applies an ACL on incoming packets</td>
</tr>
<tr>
<td>mac-access-list in</td>
<td>Uses a MAC access list</td>
</tr>
<tr>
<td>&lt;MAC-ACCESS-LIST-NAME&gt;</td>
<td>in — Applies an ACL on incoming packets</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#use mac-access-list in test
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
```

```
interface ge1
description This is \ GigabitEthernet\ 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
spanning-tree guard root
spanning-tree mst 2 port-priority 10
dot1x supplicant username Bob password 0 company@123
ip dhcp trust
ip arp header-mismatch-validation
gos trust dscp
gos trust 802.1p
channel-group 1
```

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Related Commands

- **no** — Disassociates the IP access list or MAC access list from the interface
7.1.31.3 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-rfs7000<DEVICE-RPFILEPROFILE-NAME>)#interface
[<INTERFACE-NAME>|fe <1-4>|ge <1-8>|mel|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
```

Table 7.16 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</td>
<td>page 7-175</td>
</tr>
<tr>
<td>description</td>
<td>Defines the VLAN interface description</td>
<td>page 7-176</td>
</tr>
<tr>
<td>dhcp</td>
<td>Defines DHCP settings</td>
<td>page 7-177</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 7-178</td>
</tr>
<tr>
<td>ip</td>
<td>Configures Internet Protocol (IP) config commands</td>
<td>page 7-179</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 7-182</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down an interface</td>
<td>page 7-185</td>
</tr>
<tr>
<td>use</td>
<td>Defines the settings used with this command</td>
<td>page 7-186</td>
</tr>
</tbody>
</table>
7.1.31.3.1 crypto

 Sets encryption module for this VLAN interface. The encryption module (crypto map) is configured using the crypto map command. For more information, see crypto.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
crypto map <CRYPTO-MAP-NAME>
```

**Parameters**
- crypto map `<CRYPTO-MAP-NAME>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto map </code>&lt;CRYPTO-MAP-NAME&gt;`</td>
<td>Attaches a crypto map to the selected VLAN interface. The crypto map should be existing and configured.</td>
</tr>
<tr>
<td><code>&lt;CRYPTO-MAP-NAME&gt;</code></td>
<td>Specify the crypto map name.</td>
</tr>
</tbody>
</table>

**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
## 7.1.31.3.2 description

- **interface-config-vlan-instance**

Defines a VLAN interface description. Use this command to provide additional information about the VLAN.

Supported in the following platforms:
- Access Points — AP300, 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, 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"
```

```
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
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

**Related Commands**

- **no**  
  Removes the VLAN interface description
7.1.31.3.3 dhcp

Defines Dynamic Host Configuration Protocol (DHCP) settings

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp client include client-identifier

Parameters

- dhcp client include client-identifier

| dhcp client include client-identifier | Enables sending client-identifier details in the dhcp client request. It is disabled by default |

Examples

ap8lx-4B6C00(config-device-FC-0A-81-4B-6C-00-if-vlan1)#dhcp ?
ap8lx-4B6C00(config-device-FC-0A-81-4B-6C-00-if-vlan1)#dhcp client ?
ap8lx-4B6C00(config-device-FC-0A-81-4B-6C-00-if-vlan1)#dhcp client include ?
ap8lx-4B6C00(config-device-FC-0A-81-4B-6C-00-if-vlan1)#dhcp client include client-identifier
7.1.31.3.4 dhcp-relay-incoming

 Allows an onboard DHCP server to respond to relayed DHCP packets

Supported in the following platforms:

- Access Points — AP300, 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, 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

| no | Disables or reverts interface VLAN settings to their default |
7.1.31.3.5 ip

Configures the VLAN interface’s IP settings

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

### Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip [address</td>
<td>dhcp</td>
</tr>
<tr>
<td><code>ip helper-address &lt;IP&gt;</code></td>
<td>Enables DHCP and BOOTP forwarding for a set of clients. Configures a helper address on the VLAN interface connected to the client. The helper address should specify the address of the BOOTP or DHCP servers. If you have multiple servers, configure one helper address for each server.</td>
</tr>
<tr>
<td>`ip address [&lt;IP/M&gt;</td>
<td>dhcp</td>
</tr>
<tr>
<td>`ip address [&lt;IP/M&gt; {secondary}</td>
<td>zeroconf {secondary}]`</td>
</tr>
<tr>
<td><code>ip dhcp client request options all</code></td>
<td>Uses a DHCP client to obtain an IP address for this interface</td>
</tr>
<tr>
<td>`ip nat [inside</td>
<td>outside]`</td>
</tr>
<tr>
<td>`ip ospf [authentication</td>
<td>authentication-key</td>
</tr>
<tr>
<td>`ip ospf authentication [message-digest</td>
<td>null</td>
</tr>
<tr>
<td>`ip ospf authentication-key simple-password [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]`</td>
</tr>
<tr>
<td>`ip ospf [bandwidth &lt;1-10000000&gt;</td>
<td>cost &lt;1-65535&gt;</td>
</tr>
<tr>
<td>`ip ospf message-digest-key key-id &lt;1-255&gt; md5 [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]`</td>
</tr>
</tbody>
</table>

### Parameters

- **helper-address <IP>** Enables DHCP and BOOTP forwarding for a set of clients. Configures a helper address on the VLAN interface connected to the client. The helper address should specify the address of the BOOTP or DHCP servers. 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>|dhcp|zerconf] {secondary}|zeroconf {secondary}]** Sets the VLAN interface IP address. Specifies the interface IP address in the A.B.C.D/M format. If you have multiple servers, configure one helper address for each server.
  - `<IP>` – Specify the IP address of the DHCP or BOOTP server.
  - `{secondary}` – Optional. Sets the specified IP address as a secondary address

- **dhcp** Uses a DHCP client to obtain an IP address for this interface

- **zerconf {secondary}** Uses Zero Configuration Networking (zerconf) to generate an IP address for this interface. If you have multiple servers, configure one helper address for each server.
  - `{secondary}` – Optional. Sets the generated IP address as a secondary address

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Uses a DHCP client to configure a request on this VLAN interface</td>
</tr>
<tr>
<td>client</td>
<td>Configures a DHCP client</td>
</tr>
<tr>
<td>request</td>
<td>Configures DHCP client request</td>
</tr>
<tr>
<td>options</td>
<td>Configures DHCP client request options</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>all</td>
<td>Configures all DHCP client request options</td>
</tr>
<tr>
<td>**ip nat [inside</td>
<td>outside]**&lt;br&gt;nat [inside</td>
</tr>
<tr>
<td>**ip ospf authentication [message-digest</td>
<td>null</td>
</tr>
<tr>
<td>message-digest</td>
<td>Configures md5 based authentication</td>
</tr>
<tr>
<td>null</td>
<td>No authentication required</td>
</tr>
<tr>
<td>simple-password</td>
<td>Configures simple password based authentication</td>
</tr>
<tr>
<td>**ip ospf authentication-key simple-password [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]**&lt;br&gt;ospf authentication-key</td>
</tr>
<tr>
<td>simple-password [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]</td>
</tr>
<tr>
<td>**ip ospf [bandwidth &lt;1-10000000&gt;</td>
<td>cost &lt;1-65535&gt;</td>
</tr>
<tr>
<td>cost &lt;1-65535&gt;</td>
<td>Configures OSPF cost&lt;br&gt;- &lt;1-65535&gt; – Specify OSPF cost value from 1 - 65535.</td>
</tr>
<tr>
<td>priority &lt;0-255&gt;</td>
<td>Configures OSPF priority&lt;br&gt;- &lt;0-255&gt; – Specify OSPF priority value from 0 - 255.</td>
</tr>
<tr>
<td>**ip ospf message-digest-key key-id &lt;1-255&gt; md5 [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]**&lt;br&gt;ospf message-digest</td>
</tr>
<tr>
<td>key-id &lt;1-255&gt;</td>
<td>Configures message digest authentication key ID from 0 - 255.</td>
</tr>
<tr>
<td>md5 [0 &lt;WORD&gt;</td>
<td>2 &lt;WORD&gt;]</td>
</tr>
</tbody>
</table>
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 |
7.1.31.36 no

(interface-config-vlan-instance)

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [crypto|description|dhcp-relay-incoming|ip|shutdown|use]
no [crypto map|description|dhcp-relay-incoming|shutdown|use <IP-ACCESS-LIST-NAME> in]
no ip [address|dhcp|helper-address|nat|ospf]
no ip [helper-address <IP>|nat]
no ip address [<IP/M> {secondary}|dhcp|zerconf {secondary}]
no ip dhcp client request options all
no ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|priority]

Parameters

- no [crypto map|description|dhcp-relay-incoming|shutdown|use <IP-ACCESS-LIST-NAME> in] Disassociates a crypto map from an interface
- no description Removes the VLAN interface description
- no dhcp-relay-incoming Prevents an onboard DHCP server from responding to relayed DHCP packets
- no shutdown Enables an interface
  If an interface has been shutdown, use the no shutdown command to enable the interface. Use this command to trouble shoot new interfaces.
- no use <IP-ACCESS-LIST-NAME> in Removes specified IP access list from use by an interface
  - in – Disables incoming packets
  - <IP-ACCESS-LIST-NAME> – Specify the IP access list name.
- no ip address [<IP/M> {secondary}|dhcp|zerconf {secondary}]
  Removes or reverts interface IP settings
  - address – Removes IP addresses configured for this interface
  Specify the interface IP address in the A.B.C.D/M format.
  - secondary – Optional. Removes the secondary IP address
  Removes the IP address obtained using the DHCP client
  Removes the IP address generated using a zerconf
  - secondary – Optional. Removes the secondary IP address
- **no ip address [helper-address <IP>|nat]**

<table>
<thead>
<tr>
<th>no ip address</th>
<th>Removes or reverts interface IP settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• address – Removes IP addresses configured for this interface, depending on the options used while setting the address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>helper-address &lt;IP&gt;</th>
<th>Disables the forwarding of DHCP and BOOTP packets to the configured helper IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP&gt; – Specify the IP address of the DHCP or BOOTP server.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>nat</th>
<th>Disables NAT for this interface</th>
</tr>
</thead>
</table>

- **no ip address dhcp client request options all**

<table>
<thead>
<tr>
<th>no ip address</th>
<th>Removes or reverts interface IP settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• address – Removes IP addresses configured for this interface, depending on the options used while setting the address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>dhcp</th>
<th>Removes DHCP client request configured for this interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Removes a DHCP client</td>
</tr>
<tr>
<td>request</td>
<td>Removes DHCP client request</td>
</tr>
<tr>
<td>options</td>
<td>Removes DHCP client request options</td>
</tr>
<tr>
<td>all</td>
<td>Removes all DHCP client request options</td>
</tr>
</tbody>
</table>

- **no ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|priority]**

<table>
<thead>
<tr>
<th>no ip ospf</th>
<th>Removes or reverts interface IP settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ospf – Removes OSPF settings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>authentication</th>
<th>Removes OSPF authentication scheme</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>authentication-key</th>
<th>Removes the authentication key associated with this layer 3 interface</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>bandwidth</th>
<th>Removes the bandwidth configured for the physical port mapped to this layer 3 interface</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>cost</th>
<th>Removes the OSPF cost configured for this layer 3 interface</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>message-digest-key &lt;KEY-ID&gt;</th>
<th>Removes the message digest authentication key identified by the &lt;KEY-ID&gt; keyword.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>priority</th>
<th>Removes the OSPF priority configured for this layer 3 interface</th>
</tr>
</thead>
</table>

### 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 helper-address 172.16.10.3
    ip nat inside
crypto map map1
dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)##
```
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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>Defines the encryption module</td>
</tr>
<tr>
<td>description</td>
<td>Defines the VLAN description</td>
</tr>
<tr>
<td>dhcp-relay-incoming</td>
<td>Allows an onboard DHCP server to respond to relayed DHCP packets on this interface</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP config commands</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables an interface</td>
</tr>
<tr>
<td>use</td>
<td>Defines the settings used with this command</td>
</tr>
</tbody>
</table>
7.1.31.3.7 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 — AP300, 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, 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**

```
no
```

Disables or reverts interface VLAN settings to their default
7.1.31.3.8 use

indicates config-vlan-instance

Specifies an IP access list to use with this VLAN interface

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
use [bonjour-gw-discovery-policy <POLICY-NAME>|ip-access-list in <IP-ACCESS-LIST-NAME>]

Parameters
- use [bonjour-gw-discovery-policy <POLICY-NAME>|ip-access-list in <IP-ACCESS-LIST-NAME>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bonjour-gw-discovery-policy &lt;POLICY-NAME&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>ip-access-list in &lt;IP-ACCESS-LIST-NAME&gt;</td>
<td>Uses a specified IP access list with this interface</td>
</tr>
</tbody>
</table>

Note: This feature is supported only on the RFS7000 and AP7131 devices.

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
- no | Disables or reverts interface VLAN settings to their default
7.1.31.4 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 profile > radio interface context, use the following commands:

```
<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-gain
antenna-mode
assoc-response
association-list
beacon
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
power
preamble-short
probe-response
```

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 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 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 operating
Configure the transmit power of the radio
Use short preambles on this radio
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
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 Enables 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
clrsrcl 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-71xxTestProfile-if-radio1)#

Table 7.17 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>timeout Configures adaptivity timeout on channels</td>
<td>page 7-191</td>
</tr>
<tr>
<td>aeroscout</td>
<td>Enables Aeroscout multicast packet forwarding</td>
<td>page 7-192</td>
</tr>
<tr>
<td>aggregation</td>
<td>Configures 802.11n aggregation parameters</td>
<td>page 7-193</td>
</tr>
<tr>
<td>airtime-fairness</td>
<td>Enables fair access for clients based on airtime usage</td>
<td>page 7-196</td>
</tr>
<tr>
<td>antenna-diversity</td>
<td>Transmits antenna diversity for non-11n transmit rates</td>
<td>page 7-197</td>
</tr>
<tr>
<td>antenna-downtilt</td>
<td>Enables Advanced Element Panel Technology (ADEPT) antenna mode</td>
<td>page 7-198</td>
</tr>
<tr>
<td>antenna-gain</td>
<td>Specifies the antenna gain for the selected radio</td>
<td>page 7-199</td>
</tr>
<tr>
<td>antenna-mode</td>
<td>Configures the radio antenna mode</td>
<td>page 7-200</td>
</tr>
<tr>
<td>assoc-response</td>
<td>Enables/disables an access point to ignore or respond to an association/authorization request</td>
<td>page 7-201</td>
</tr>
<tr>
<td></td>
<td>based on the configured received RSSI threshold value</td>
<td></td>
</tr>
<tr>
<td>association-list</td>
<td>Associates an existing global association list with this radio interface</td>
<td>page 7-202</td>
</tr>
<tr>
<td>beacon</td>
<td>Configures beacon parameters</td>
<td>page 7-203</td>
</tr>
<tr>
<td>channel</td>
<td>Configures a radio’s channel of operation</td>
<td>page 7-205</td>
</tr>
</tbody>
</table>
### Table 7.17  Interface-Radio-Config-Mode Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-rates</td>
<td>Specifies the 802.11 rates supported on a radio</td>
<td>page 7-206</td>
</tr>
<tr>
<td>description</td>
<td>Configures the selected radio’s description</td>
<td>page 7-210</td>
</tr>
<tr>
<td>dfs-rehome</td>
<td>Reverts to configured home channel once Dynamic Frequency Selection (DFS) evacuation period expires</td>
<td>page 7-211</td>
</tr>
<tr>
<td>dynamic-chain-selection</td>
<td>Enables automatic antenna mode selection</td>
<td>page 7-212</td>
</tr>
<tr>
<td>ekahau</td>
<td>Enables Ekahau multicast packet forwarding</td>
<td>page 7-213</td>
</tr>
<tr>
<td>extended-range</td>
<td>Configures extended range</td>
<td>page 7-214</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 7-215</td>
</tr>
<tr>
<td>guard-interval</td>
<td>Configures the 802.11n guard interval</td>
<td>page 7-216</td>
</tr>
<tr>
<td>ldpc</td>
<td>Enables support for Low Density Parity Check (LDPC) on the radio interface</td>
<td>page 7-217</td>
</tr>
<tr>
<td>lock-rf-mode</td>
<td>Retains user configured RF mode settings for the selected radio</td>
<td>page 7-218</td>
</tr>
<tr>
<td>max-clients</td>
<td>Configures the maximum number of wireless clients allowed to associate with this radio</td>
<td>page 7-219</td>
</tr>
<tr>
<td>mesh</td>
<td>Configures radio mesh parameters</td>
<td>page 7-220</td>
</tr>
<tr>
<td>meshpoint</td>
<td>Maps an existing meshpoint to this radio interface</td>
<td>page 7-222</td>
</tr>
<tr>
<td>non-unicast</td>
<td>Configures the handling of non unicast frames on this radio</td>
<td>page 7-226</td>
</tr>
<tr>
<td>off-channel-scan</td>
<td>Enables selected radio’s off channel scanning parameters</td>
<td>page 7-228</td>
</tr>
<tr>
<td>placement</td>
<td>Defines selected radio’s deployment location</td>
<td>page 7-230</td>
</tr>
<tr>
<td>power</td>
<td>Configures the transmit power on this radio</td>
<td>page 7-231</td>
</tr>
<tr>
<td>preamble-short</td>
<td>Enables the use of short preamble on this radio</td>
<td>page 7-232</td>
</tr>
<tr>
<td>probe-response</td>
<td>Configures transmission parameters for probe response frames</td>
<td>page 7-233</td>
</tr>
<tr>
<td>radio-resource-measurement</td>
<td>Enables 802.11k radio resource measurement</td>
<td>page 7-234</td>
</tr>
<tr>
<td>radio-share-mode</td>
<td>Configures the mode of operation, for this radio, as radio-share</td>
<td>page 7-235</td>
</tr>
<tr>
<td>rate-selection</td>
<td>Sets the rate selection method to standard or opportunistic</td>
<td>page 7-236</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes the radio’s channel of operation</td>
<td>page 7-237</td>
</tr>
<tr>
<td>rf-mode</td>
<td>Configures the radio’s RF mode</td>
<td>page 7-238</td>
</tr>
<tr>
<td>rifs</td>
<td>Configures Reduced Interframe Spacing (RIFS) parameters on this radio</td>
<td>page 7-240</td>
</tr>
</tbody>
</table>
### Table 7.17 Interface-Radio-Config-Mode Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>rts-threshold</td>
<td>Configures the Request to Send (RTS) threshold value on this radio</td>
<td>page 7-241</td>
</tr>
<tr>
<td>shutdown</td>
<td>Terminates or shuts down selected radio interface</td>
<td>page 7-243</td>
</tr>
<tr>
<td>smart-rf</td>
<td>Overrides Smart RF channel width setting on the selected radio</td>
<td>page 7-244</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 7-245</td>
</tr>
<tr>
<td>stbc</td>
<td>Configures radio’s Space Time Block Coding (STBC) mode</td>
<td>page 7-247</td>
</tr>
<tr>
<td>transmit-beamforming</td>
<td>Enables transmit beamforming on the selected radio interface</td>
<td>page 7-248</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 7-249</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 7-250</td>
</tr>
<tr>
<td>wireless-client</td>
<td>Configures wireless client parameters on selected radio</td>
<td>page 7-251</td>
</tr>
<tr>
<td>wlan</td>
<td>Enables a WLAN on selected radio</td>
<td>page 7-252</td>
</tr>
</tbody>
</table>
7.1.31.4.1 adaptivity timeout

> interface-config-radio-instance

Configures adaptivity timeout on channels. The channel is avoided till the adaptivity timeout expires.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP7502, AP7522, AP7532, AP82XX
- Wireless Controllers — RFS4011

Syntax
adaptivity timeout <30-3600>

Parameters
- adaptivity timeout <30-3600>

<table>
<thead>
<tr>
<th>adaptivity timeout &lt;30-3600&gt;</th>
<th>Configures adaptivity timeout on a channel. The channel is avoided till the adaptivity timeout expires. After adaptivity timeout expiry, the radio is reverted back to the original channel.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> This feature is applicable for Fixed channel only.</td>
</tr>
<tr>
<td></td>
<td>• &lt;30-3600&gt; – Specify the adaptivity time out value from 30-3600 minutes.</td>
</tr>
</tbody>
</table>

Examples
ap6522-C(config-device-B4-C7-99-63-9A-94-if-radio2)#adaptivity timeout 300

ap6522-C(config-device-B4-C7-99-63-9A-94-if-radio2)#sho context
interface radio2
 no shutdown
 channel 60
 wlan macauth bss 1 primary
 wlan adaptivity-wlan bss 2 primary
 adaptivity timeout 300
7.1.31.4.2 aeroscout

*interface-config-radio-instance*

Enables Aeroscout multicast packet forwarding. This feature is disabled by default.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP7502, AP7522, AP7532, AP82XX
- Wireless Controllers — RFS4011

**Syntax**
aeroscout [forward|mac <MAC>]

**Parameters**
- aeroscout [forward|mac <MAC>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward</td>
<td>Enables Aeroscout multicast packet forwarding</td>
</tr>
<tr>
<td>mac &lt;MAC&gt;</td>
<td>Configures the multicast MAC address to forward the packets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;</td>
<td>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 radio1
   aeroscout forward
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

**Related Commands**
- no Disables Aeroscout Multicast packet forwarding
### 7.1.31.4.3 aggregation

**Interface-config-radio-instance**

Configures 802.11n frame aggregation. 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```plaintext
aggregation [ampdu|amsdu]

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]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregation</td>
<td>Configures 802.11n frame aggregation parameters</td>
</tr>
<tr>
<td>ampdu</td>
<td>Configures <em>Aggregate MAC Protocol Data Unit</em> (AMPDU) frame aggregation parameters</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>tx-only</td>
<td>Supports the transmission of AMPDU aggregated frames only</td>
</tr>
<tr>
<td>rx-only</td>
<td>Supports the receipt of AMPDU aggregated frames only</td>
</tr>
<tr>
<td>tx-rx</td>
<td>Supports the transmission and receipt of AMPDU aggregated frames (default setting)</td>
</tr>
<tr>
<td>none</td>
<td>Disables support for AMPDU aggregation</td>
</tr>
</tbody>
</table>

- **aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregation</td>
<td>Configures 802.11n frame aggregation parameters</td>
</tr>
<tr>
<td>ampdu</td>
<td>Configures AMPDU frame aggregation parameters</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>max-aggr-size</td>
<td>Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.</td>
</tr>
</tbody>
</table>
### aggreation ampdu max-aggr-size tx <2000-65535>

**rx**

- [8191|16383|32767|65535]
  - Configures the limit on 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**

- 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.

**max-aggr-size**

- Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.

**tx <2000-65535>**

- Configures the maximum size (in bytes) for AMPDU aggregated transmitted frames
  - **<2000-65535>** – Sets the limit from 2000 - 65535 bytes. The default is 65535 bytes.

**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.

**mn-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 (default setting)
  - **8** – Configures the minimum gap as 8 microseconds
  - **16** – Configures the minimum gap as 16 microseconds

**aggregation**

- Configures 802.11n frame aggregation parameters

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables 802.11n aggregation parameters</td>
</tr>
</tbody>
</table>
7.1.31.4.4 airtime-fairness

**interface-config-radio-instance**

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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>airtime-fairness</td>
<td>Enables fair access to the medium for wireless clients based on their airtime usage</td>
</tr>
<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>&lt;1-10&gt;</td>
<td>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` | Disables fair access for wireless clients (provides access on a round-robin mode)
7.1.31.4.5 antenna-diversity

```interface-config-radio-instance```

Configures 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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
```

| no | Uses single antenna for non-11n transmit rates |
7.1.31.4.6 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 — AP71XX

**NOTE:** This feature is not supported on AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, and RFS4011.

**Syntax**

antenna-downtilt

**Parameters**

None

**Examples**

```bash
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
  aeroscout 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>
7.1.31.4.7 antenna-gain

Configures 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
antenna-gain <0.0-15.0>

Parameters
- antenna-gain <0.0-15.0>

| <0.0-15.0> | Sets the antenna gain from 0.0 - 15.0 dBi. The default 0.00. |

Examples
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
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands
- no
  Resets the radio's antenna gain parameter
### 7.1.31.4.8 antenna-mode

CONFIGURES THE ANTENNA MODE (THE NUMBER OF TRANSMIT AND RECEIVE ANTENNAS) ON THE RADIO

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. The default setting is dynamic based on the access point model deployed and its transmit power settings.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
antenna-mode [1*1|1*ALL|2*2|default]
```

**Parameters**

- `antenna-mode [1*1|1*ALL|2*2|default]`

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</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 antenna A 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 1x1.

**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 ampdu tx-only
   aeroscout forward
   antenna-mode 2x2
   antenna-diversity
   airtime-fairness prefer-ht weight 6
   antenna-downtilt
```

**Related Commands**

- `no`
  Resets the radio antenna mode (the number of transmit and receive antennas) to its default
### 7.1.31.4.9 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
assoc-response rssi-threshold <-128--40>
```

**Parameters**

- `assoc-response rssi-threshold <-128--40>`

**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
rfs7000-37FABE(config-profile-71XXTestProfile-if-radio1)#
```

**Related Commands**

```
no
```

Removes the RSSI threshold, based on which an association/authorization request is either ignored or responded.
7.1.31.4.10 association-list

*interface-config-radio-instance*

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, 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the global association list associated with this radio interface</td>
</tr>
</tbody>
</table>
7.1.31.4.11 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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 <1-8> <1-50]**
  - Configures the radio DTIM interval. A DTIM is a message that informs wireless clients about the presence of buffered multicast or broadcast data. The message is generated within the periodic beacon at a frequency specified by the DTIM interval.
  - `<1-50>` Configures a single value to use on the radio. Specify a value between 1 and 50.
  - `bss <1-16> <1-50>` Configures a separate DTIM for a Basic Service Set (BSS) on a radio
    - `<1-16>` – Sets the BSS number from 1 - 16
    - `<1-50>` – Sets the BSS DTIM from 1 - 50

- **beacon period [50|100|200]**
  - Configures the beacon period (the interval between consecutive radio beacons)
    - 50 – Configures 50 K-uSec interval between beacons
    - 100 – Configures 100 K-uSec interval between beacons (default)
    - 200 – Configures 200 K-uSec interval between beacons

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#beacon dtim-period bss 2 20
rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#beacon period 50

rfs7000-37FABE(config-profile-71xxTestProfile-if-radiol)#show context
interface radiol
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
--More--
### Related Commands

| no               | Removes the configured beacon parameters |
7.1.31.4.12 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 AP8232, and are unique to the 80 MHz band.

---

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
channel [smart|acs|1|2|3|4|-------]
```

**Parameters**

- `channel [smart|acs|1|2|3|4|-------]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`smart</td>
<td>acs</td>
</tr>
<tr>
<td>smart</td>
<td>Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled). This is the default setting.</td>
</tr>
<tr>
<td>acs</td>
<td>Uses automatic channel selection (ACS) to assign a channel</td>
</tr>
<tr>
<td>1</td>
<td>Channel 1 in 20 MHz</td>
</tr>
<tr>
<td>2</td>
<td>Channel 1 in 20 MHz</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#channel 1
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
  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--
```

**Related Commands**

```
no | Resets a radio’s channel of operation
```
7.1.31.4.13 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>b-only</th>
<th>Supports operation in the 802.11b mode only (applicable for 2.4 and 4.9 GHz bands)</th>
</tr>
</thead>
<tbody>
<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>Option</td>
<td>Description</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>
</tbody>
</table>

- **data-rates custom**
  - 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 rates for both with and without short guard intervals (SGI).
- `data-rates mcs qam-only`

| mcs qam-only | Configures supports for MCS QAM data rates only |

**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 With 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

```
rf7000-37FABE(config-profile-71xxTestProfile-if-radio1)#data-rates b-only
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
data-rates b-only
channel 1
  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
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
--More--
```

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

- `no` Resets the 802.11 data rates on a radio
- `rf-mode` Configures the radio’s RF mode of operation
7.1.31.4.14 description

- **interface-config-radio-instance**

Configures the selected radio's description

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

description <WORD>

**Parameters**
- description <WORD>

<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Defines a description for the selected radio (should not exceed 64 characters in length)</th>
</tr>
</thead>
</table>

**Examples**

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 |
### 7.1.31.4.15 dfs-rehome

- **interface-config-radio-instance**

  Reverts to configured home channel once the Dynamic Frequency Selection (DFS) evacuation period expires.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

dfs-rehome

**Parameters**
None

**Examples**

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#dfs-rehome

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>Stays on DFS elected channel after evacuation period expires</td>
</tr>
</tbody>
</table>
7.1.31.4.16 dynamic-chain-selection

Enables automatic antenna mode selection (single antenna for non-11n transmit rates). This option is enabled by default.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

dynamic-chain-selection

Parameters
None

Examples
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#dynamic-chain-selection
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#

Related Commands

| no | Uses the configured transmit antenna mode for all clients |
**7.1.31.4.17 ekahau**

> **interface-config-radio-instance**

Enables Ekahau multicast packet forwarding

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
ekahau [forward|mac <MAC>]
```

```
ekahau forward ip <IP> port <0-65535>
```

**Parameters**

- `ekahau [forward|mac <MAC>]`

<table>
<thead>
<tr>
<th>Forward ip &lt;IP&gt; port &lt;0-65535&gt;</th>
<th>Enables multicast packet forwarding to the Ekahau engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip <code>&lt;IP&gt;</code></td>
<td>Configures the IP address of the Ekahau engine in the A.B.C.D format</td>
</tr>
<tr>
<td>port <code>&lt;0-65535&gt;</code></td>
<td>Specifies the TaZman Sniffer Protocol (TZSP) port on Ekahau engine from 0 - 65535</td>
</tr>
<tr>
<td>TZSP is an encapsulation protocol, which is generally used to wrap 802.11 wireless packets.</td>
<td></td>
</tr>
</tbody>
</table>

- `mac <MAC>`

<table>
<thead>
<tr>
<th>mac <code>&lt;MAC&gt;</code></th>
<th>Configures the multicast MAC address to forward the packets</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>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)#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 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
  --More--
```

**Related Commands**

| no | Uses default Ekahau multicast MAC address |
7.1.31.4.18 extended-range

```
interface-config-radio-instance
```

Configures the extended range capability for AP71XX model devices

Supported in the following platforms:
- Access Point — AP71XX, AP81XX

**Syntax**

```
extended-range <1-25>
```

**Parameters**

- extended-range <1-25>

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#extended-range
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
```

```
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

```
no
```

Resets the extended range to default (7 km for 2.4 GHz and 5 km for 5.0 GHz)
7.1.31.4.19 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, 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...............]`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| fallback-channel [100|100w|100ww|104|104w|104ww|108|108w...............] | 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the fallback-channel configuration</td>
</tr>
</tbody>
</table>
7.1.31.4.20 guard-interval

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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

```
guard-interval [any|long]
```

Parameters

- `guard-interval [any|long]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>any</code></td>
<td>Enables the radio to use any short (400nSec) or long (800nSec) guard interval</td>
</tr>
<tr>
<td><code>long</code></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
```

Related Commands

```
no
```

Resets the 802.11n guard interval to default (long: 800nSec)
7.1.3.1.4.21 ldpc

*interface-config-radio-instance*

Enables support for *Low Density Parity Check* (LDPC) on the radio interface.

LDPC consists of forward error correcting codes that enable error control in data transmission.

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX
- Wireless Controllers — RFS4011

**Syntax**

`ldpc`

**Parameters**

None

**Examples**

```
rfs4000-229D58(config-profile-Test81XX-if-radio1)#ldpc
rfs4000-229D58(config-profile-Test81XX-if-radio1)#
rfs4000-229D58(config-profile-Test81XX-if-radio1)#show context interface radio1 ldpc
rfs4000-229D58(config-profile-Test81XX-if-radio1)#
```

**Related Commands**

- `no` Disables LDPC support
7.1.31.4.22 lock-rf-mode

**interface-config-radio-instance**

Retains user configured RF mode settings for the selected radio

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Allows Smart RF to change a radio’s RF mode settings</td>
</tr>
</tbody>
</table>
7.1.31.4.23 max-clients

**interface-config-radio-instance**

Configures the maximum number of wireless clients allowed to associate with this radio

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```plaintext
max-clients <0-256>
```

**Parameters**

- `max-clients <0-256>`

<table>
<thead>
<tr>
<th><code>&lt;0-256&gt;</code></th>
<th>Configures the maximum number of clients allowed to associate with a radio. Specify a value from 0 - 256. The default is 256.</th>
</tr>
</thead>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#max-clients 100
```

```plaintext
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**

| `no` | Resets the maximum number of wireless clients allowed to associate with a radio |
7.1.31.4.24 mesh

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.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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 <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2 <LINE>|<LINE>]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mesh</td>
<td>Configures radio mesh parameters, such as maximum number of mesh links, preferred peer device, client operations etc.</td>
</tr>
<tr>
<td>client</td>
<td>Enables operation as a client (scans for mesh portals or nodes that have connectivity to portals and connects through them)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>links &lt;1-6&gt;</td>
<td>Configures the maximum number of mesh links a radio attempts to create</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-6&gt; — Sets the maximum number of mesh links from 1 - 6. The default is 3.</td>
</tr>
<tr>
<td>portal</td>
<td>Enables operation as a portal (begins beaconing immediately, accepting connections from other mesh nodes, typically the node with a connection to the wired network)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>preferred-peer &lt;1-6&gt; &lt;MAC&gt;</td>
<td>Configures a preferred peer device</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-6&gt; — Configures the priority at which the peer node will be added</td>
</tr>
<tr>
<td></td>
<td>When connecting to the mesh infrastructure, nodes with lower priority are given precedence over nodes with higher priority.</td>
</tr>
<tr>
<td></td>
<td>• &lt;MAC&gt; — Sets the MAC address of the preferred peer device (Ethernet MAC of either a AP, wireless controller, or service platform with onboard radios)</td>
</tr>
<tr>
<td>psk [0 &lt;LINE&gt;</td>
<td>2 &lt;LINE&gt;</td>
</tr>
<tr>
<td></td>
<td>• 0 &lt;LINE&gt; — Enter a clear text key</td>
</tr>
<tr>
<td></td>
<td>• 2 &lt;LINE&gt; — Enter an encrypted key</td>
</tr>
<tr>
<td></td>
<td>• &lt;LINE&gt; — Enter the pre-shared key</td>
</tr>
<tr>
<td></td>
<td>Pre-shared keys should be 8 - 64 characters in length.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables mesh mode operation of the selected radio</td>
</tr>
</tbody>
</table>
### 7.1.31.4.25 meshpoint

- **interface-config-radio-instance**

Maps an existing meshpoint to this radio

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
meshpoint <MESHPOINT-NAME> {bss <1-16>}
```

**Parameters**

- **meshpoint <MESHPOINT-NAME> {bss <1-16>}**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint &lt;MESHPOINT-NAME&gt;</td>
<td>Maps a meshpoint to this radio. Specify the meshpoint name.</td>
</tr>
<tr>
<td>bss &lt;1-16&gt;</td>
<td>Optional. Specifies the radio’s BSS where this meshpoint is mapped</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-16&gt; – Specify the BSS number from 1 - 16.</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
                   meshpoint test bss 7
rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#
```

**Related Commands**

- **no** Disables meshpoint on the selected radio
7.1.31.4.26 no

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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
no <PARAMETERS>

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-profile-ap71xxTest-if-radio1)#no ?
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-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
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
The following example shows radio interface settings before the 'no' commands are executed:

rfs7000-37FABE(config-profile-ap71xxTest-if-radio1)#

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 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)#
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 ampdu 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)#
### 7.1.31.4.27 non-unicast

**interface-config-radio-instance**

Configures the support for non unicast frames on this radio. Enables the forwarding of multicast and broadcast frames by this radio.

Supported in the following platforms:

- **Access Points** — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- **Wireless Controllers** — RFS4011

**Syntax**

```plaintext
non-unicast [forwarding|queue|tx-rate]
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 [follow-dtim|power-save-aware]**
  - `forwarding` Configures support for non unicast frames
  - `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 if all associated wireless clients are in the power save mode

- **non-unicast queue [<1-200>|bss <1-16> <1-200>]**
  - `queue` Configures the number of broadcast packets queued per BSS on this radio. This command also enables you to override the default on a specific BSS.
  - `<1-200>` Specify a number from 1 - 200.
  - `bss <1-16> <1-200>` Overrides the default on a specified BSS
    - `<1-16>` – Select the BSS to override the default.
    - `<1-200>` – Specify the number of broadcast packets queued for the selected BSS.

- **non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]**
  - `tx-rate` Configures the transmission data rate for broadcast and multicast frames
  - `bss <1-16>` Overrides the default on a specified BSS
    - `<1-16>` – Select the BSS to override the default.
  - `dynamic-all` Dynamically selects a rate from all supported rates based on current traffic conditions
  - `dynamic-basic` Dynamically selects a rate from all supported basic rates based on current traffic conditions
### Examples

```
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 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
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

| **no** | Resets the handling of non unicast frames to its default |
7.1.31.4.28 off-channel-scan

- interface-config-radio-instance

Enables selected radio’s off channel scanning parameters. This option is disabled by default.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>}

  off-channel-scan Enables off channel scanning parameters. These parameters are optional, and the system configures default settings if no values are specified.

  channel-list [2.4GHz|5GHz] Optional. Specifies the channel list to scan
  - 2.4GHz – Selects the 2.4 GHz band
  - 5GHz – Selects the 5.0 GHz band

  <CHANNEL-LIST> Optional. Specifies a list of 20 MHz or 40 MHz channels for the selected band (the channels are separated by commas or hyphens)

- off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}

  off-channel-scan Enables off-channel scanning on this radio. These parameters are optional, and the system configures default settings if no values are specified.

  max-multicast <0-100> Optional. Configures the maximum multicast/broadcast messages 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 10 dtims.

- off-channel-scan {sniffer-redirect tzsp <IP>}

  off-channel-scan Enables off channel scanning parameters. These parameters are optional, and the system configures default settings if no values are specified.

  sniffer-redirect tzsp <IP> Optional. Captures and redirects packets to an IP address running a packet capture analysis tool
  - tzsp – Encapsulates captured packets in TZSP before redirecting
  - <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><code>no</code></td>
<td>Disables radio off channel scanning</td>
</tr>
</tbody>
</table>
7.31.4.29 placement

*interface-config-radio-instance*

Defines the location where the radio is deployed. 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

placement [indoor|outdoor]

**Parameters**

- placement [indoor|outdoor]

<table>
<thead>
<tr>
<th>indoor</th>
<th>Radio is deployed indoors (uses indoor regulatory rules). This is the default setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>outdoor</td>
<td>Radio is deployed outdoors (uses outdoor regulatory rules)</td>
</tr>
</tbody>
</table>

**Examples**

```shell
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#placement outdoor
```

```shell
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
```

```shell
--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>Resets a radio’s deployment location</td>
</tr>
</tbody>
</table>
### 7.1.31.4.30 power

#### interface-config-radio-instance

Configures a 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

#### Syntax

```
power [<1-30>|smart]
```

#### Parameters

- **power [<1-30>|smart]**

#### 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
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
```

#### Related Commands

- **no**
  Resets a radio’s transmit power
7.1.31.4.31 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>no</td>
<td>Disables the use of short preamble on a radio</td>
</tr>
</tbody>
</table>
7.1.31.4.32 probe-response

`interface-config-radio-instance`

Configures transmission parameters for probe response frames

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
probe-response [rate|retry]
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

**Parameters**

- `probe-response retry`

  - `retry`
    
    Retransmits probe response if no acknowledgement is received from the client. This option is enabled by default.

- `probe-response rate [follow-probe-request|highest-basic|lowest-basic]`

  - `rate`
    
    Configures data transmission rates used for the transmission of probe responses
  
  - `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

**Examples**

```
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#probe-response rate follow-probe-request
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

**Related Commands**

```
no
```

Resets transmission parameters for probe response frames
7.1.31.4.33 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>
</table>
| attenuation-threshold <1-199> | Configures the neighbor attenuation threshold, considered when generating channel and neighbor reports  
|                    | • <1-199> — Specify the attenuation threshold from 1 -199.                                                                                                                                                   |
| max-entries <1-12>   | Configures the maximum number of entries to include in channel and neighbor reports  
|                    | • <1-12> — Specify a value from 1 - 12.                                                                                                                                                                      |

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)#
```

```
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)#
```

```
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
7.1.31.4.34 radio-share-mode

Configure a 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
radio-share-mode [inline|off|promiscuous]

Parameters
- radio-share-mode [inline|off|promiscuous]

<table>
<thead>
<tr>
<th>radio-share-mode</th>
<th>Configure the Radio Share mode of operation. The options are: inline, off, and promiscuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>inline</td>
<td>Enables sharing of all WLAN packets (matching the BSSID of the radio) serviced by the radio. In the inline mode, all packets are shared with the WIPS sensor module.</td>
</tr>
<tr>
<td>off</td>
<td>Disables Radio Share (no packets shared with WIPS sensor module)</td>
</tr>
<tr>
<td>promiscuous</td>
<td>Enables the sharing of packets received in the promiscuous mode (i.e. without filtering based on BSSID). In the promiscuous mode, the radio captures every frame it sees on the channel it is set for.</td>
</tr>
</tbody>
</table>

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
### 7.1.31.4.35 rate-selection

Sets the rate selection method to standard or opportunistic

**Syntax**

```
rate-selection [opportunistic|standard]
```

**Parameters**

- **rate-selection [opportunistic|standard]**
- **standard**
  - Configures the monotonic rate selection mode. This is the default setting.
- **opportunistic**
  - Configures the opportunistic (ORLA) rate selection mode
  - 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**

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rate-selection opportunistic
%% Error: Rate selection cannot be changed for device [rfs4000]
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

**Related Commands**

- **no**
  - Resets the rate selection mode to standard (monotonic)
7.1.31.4.36 remove-override

`interface-config-radio-instance`

Removes the radio’s channel of operation

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

`remove-override channel`

**Parameters**

- `remove-override channel`

---

**Examples**

```
rfs4000-229D58 (config-profile-testRFS4000-if-radio1)#show context
  interface radio1
  channel 9
rfs4000-229D58 (config-profile-testRFS4000-if-radio1)#

rfs4000-229D58 (config-profile-testRFS4000-if-radio1)#remove-override channel

rfs4000-229D58 (config-profile-testRFS4000-if-radio1)#show context
  interface radio1
rfs4000-229D58 (config-profile-testRFS4000-if-radio1)#
```
7.1.31.4.3 rf-mode

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 radio.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|client-bridge|scan-ahead|sensor]
```

**Parameters**

- **rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|client-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>client-bridge</td>
<td>Enables this radio to operate as a client bridge radio</td>
</tr>
<tr>
<td>scan-ahead</td>
<td>Enables this radio to operate as a scan-ahead radio</td>
</tr>
<tr>
<td>A radio functioning in the scan-ahead mode is used for forward scanning only. The radio does not support WLAN or Mesh services.</td>
<td></td>
</tr>
<tr>
<td>sensor</td>
<td>Operates as a sensor radio. Configures this radio to function as a scanner, providing scanning services on both 2.4 GHz and 5.0 GHz bands. The radio does not provide WLAN services.</td>
</tr>
</tbody>
</table>

The scan ahead feature is used in Dynamic Frequency Selection (DFS) aware countries for infrastructure devices, static, and vehicular mounted modems (VMMs). It enables a secondary radio to scan ahead for an active channel for backhaul transmission, in the event of a radar trigger on the primary radio. The device then switches radios allowing transmission to continue. This is required in environments where handoff is required and DFS triggers are common.

With a secondary radio dedicated for forward scanning, the primary radio, in case of radar hit, hands over the channel availability check (CAC) function to the secondary radio. This avoids a break in data communication, which would have resulted if the primary radio was to do CAC itself.

The secondary radio periodically does a scan of the configured channel list, searching for the other available meshpoint roots. When configured on the root meshpoint, the scan-ahead feature also scans for cleaner channels.
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>
### 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.

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>rifs</th>
<th>Configures RIFS parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Disables support for RIFS</td>
</tr>
<tr>
<td></td>
<td>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
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
--More--
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

#### Related Commands

- **no** Disables radio's RIFS parameters
7.1.31.4.39 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

```plaintext
rts-threshold <0-65536>
```

Parameters

- `<0-65536>` Specify the RTS threshold value from 0-65536 bytes.

Examples

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#rts-threshold 100
```

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
```

```plaintext
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
  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--
```

```plaintext
rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

- `no` Resets a radio’s RTS threshold to its default
7.1.31.4.40 service

**interface-config-radio-instance**

Enables/disables 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**

```plaintext
service radio-lna [agc|ms]
```

**Parameters**

- `service radio-lna [agc|ms]`

| radio-lna [agc|ms] | Enables/disables dynamic control function |
|--------------------|------------------------------------------|
|                    | • agc – Enables dynamic LNA control function. This is the default setting. |
|                    | • ms – Disables dynamic LNA control function |

**Examples**

```plaintext
nx9500-6C8809(config-profile-testAP6522-if-radio1)#service radio-lna ms
```

```plaintext
nx9500-6C8809(config-profile-testAP6522-if-radio1)#show context
  interface radio1
  service radio-lna ms
  nx9500-6C8809(config-profile-testAP6522-if-radio1)#
```

**Related Commands**

```plaintext
no
```

Reverts radio-lna mode to default (agc)
7.1.31.4.41 shutdown

Terminates or shuts down selected radio interface

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>no</td>
<td>Enables a disabled radio interface</td>
</tr>
</tbody>
</table>
7.1.31.4.42 smart-rf

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, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax
smart-rf preferred-channel-width [20MHz|40MHz|80MHz]

Parameters
- smart-rf preferred-channel-width [20MHz|40MHz|80MHz]

| smart-rf preferred-channel-width [2-MHz|40MHz|80MHz] | Configures the preferred channel width. The options are: |
|-----------------------------------------------------|----------------------------------------------------------|
| • 20MHz – Sets 20 MHz as the preferred channel of operation |
| • 40MHz – Sets 40MHz as the preferred channel of operation |
| • 80MHz – Sets 80MHz as the preferred channel of operation (default setting) |

Examples
nx9500-6C8809(config-profile-testAP71XX-if-radio1)#smart-rf preferred-channel-width 40MHz

nx9500-6C8809(config-profile-testAP71XX-if-radio1)#show context interface radio1
smart-rf preferred-channel-width 40MHz
rate-selection opportunistic
nx9500-6C8809(config-profile-testAP71XX-if-radio1)#

Related Commands
- no Enables use of Smart RF selected channel of operation
7.1.31.4.43 sniffer-redirect

Captures and redirects packets to an IP address running a packet capture/analysis tool

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>omnipeek</td>
<td>Encapsulates captured packets in proprietary header (use 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></td>
<td>• 1 – Channel 1 in 20 MHz mode (default setting)</td>
</tr>
<tr>
<td></td>
<td>• 10 – Channel 10 in 20 MHz mode</td>
</tr>
<tr>
<td></td>
<td>• 100 – Channel 100 in 20 MHz mode</td>
</tr>
<tr>
<td></td>
<td>• 100w – Channels 100w in 40 MHz mode (channels 100*,104)</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></td>
<td>• &lt;1-65535&gt; – Specify the maximum truncated byte length of captured packets</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-radio1)#sniffer-redirect omnipeek
172.16.10.1 channel 1
```
```
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
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables packet capture and redirection</td>
</tr>
</tbody>
</table>
7.1.3.1.44 stbc

- interface-config-radio-instance

Configures 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

stbc [none|tx-only]

**Parameters**

- stbc [none|tx-only]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Disables STBC support (default setting)</td>
</tr>
<tr>
<td>tx-only</td>
<td>Configures the AP radio to format and broadcast the special stream (enables STBC support for transmit only)</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#stbc tx-only
rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#show context interface radio1
  stbc tx-only
rfs7000-37FABE(config-profile-81xxTestProfile-if-radio1)#
```

**Related Commands**

- no
  - Disables STBC support
7.1.31.4.45 transmit-beamforming

*interface-config-radio-instance*

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 — AP7522, AP7532, AP8132

**Syntax**

transmit-beamforming enable

**Parameters**
- transmit-beamforming enable

| transmit-beamforming enable | Enables transmit-beamforming feature. By default this feature is disabled. |

**Examples**

```
rfs6000-81742D(config-profile-testAP7522-if-radio1)#transmit-beamforming
rfs6000-81742D(config-profile-testAP7522-if-radio1)#show context
   interface radio1
        transmit-beamforming
rfs6000-81742D(config-profile-testAP7522-if-radio1)#
```

**Related Commands**

| no | Disables transmit beamforming feature |
7.1.31.4.46 use

`interface-config-radio-instance`

Enables an association ACL policy and a radio QoS policy for 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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>association-acl-policy</th>
<th>Uses a specified association ACL policy with this radio interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;ASSOC-ACL-POLICY-NAME&gt;</code> – Specify the association ACL policy name (should be existing and fully configured).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>radio-qos-policy</th>
<th>Uses a specified radio QoS policy with this radio interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;RADIO-QoS-POLICY-NAME&gt;</code> – Specify the radio QoS policy name (should be existing and fully configured).</td>
</tr>
</tbody>
</table>

Examples

```
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
  rfs-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

`no` | Dissociates the specified association ACL policy and radio QoS policy
### 7.1.31.4.47 wips

**interface-config-radio-instance**

Enables access point to change its channel of operation in order to terminate rogue devices. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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 to enable them perform rogue detection and termination.

### Syntax

```text
wips airtime-termination allow-channel-change
```

### Parameters

- `wips airtime-termination allow-channel-change` Enables access point to change its channel of operation in order to terminate rogue devices

### Examples

```text
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
7.1.31.4.48 wireless-client

> interface-config-radio-instance

Configures wireless client parameters on this radio

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

Syntax

wireless-client tx-power [<0-20>|mode]

wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]

Parameters

- wireless-client tx-power <0-20>
- wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]

Examples

rfs7000-37FABE(config-profile-71xxTestProfile-if-radio1)#wireless-client tx-power 20

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
  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
  --More--

Related Commands

no

Resets the transmit power indicated to wireless clients
7.1.31.4.49 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 — AP300, AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4011

**Syntax**

```
wlan <WLAN-NAME> {bss|primary}
```

```
wlan <WLAN-NAME> {bss <1-8> |primary}
```

**Parameters**
- `wlan <WLAN-NAME> {bss <1-8> |primary}`
  - `<WLAN-NAME>` Specify the WLAN name (it must have been already created and configured)
  - `bss <1-8>` — Optional. Specifies a BSS for the radio to map the WLAN
    - `<1-8>` — Specify the BSS number from 1 - 8.
  - `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
  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
7.1.31.5 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, 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.

Table 7.18 summarizes WWAN interface configuration commands.

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>apn</code></td>
<td>Configures the access point’s name provided by the service provider</td>
<td>page 7-255</td>
</tr>
<tr>
<td><code>auth-type</code></td>
<td>Configures the authentication types used on this interface</td>
<td>page 7-256</td>
</tr>
<tr>
<td><code>crypto</code></td>
<td>Associates a crypto map with this interface</td>
<td>page 7-257</td>
</tr>
</tbody>
</table>
Table 7.18  Interface-Config-WWAN1-Interface Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Configures a unique description for this interface</td>
<td>page 7-258</td>
</tr>
<tr>
<td>ip</td>
<td>Associates an IP ACL with this interface</td>
<td>page 7-259</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the WWAN interface settings</td>
<td>page 7-260</td>
</tr>
<tr>
<td>password</td>
<td>Configures a password for this WWAN interface</td>
<td>page 7-261</td>
</tr>
<tr>
<td>use</td>
<td>Associates an IP ACL with this interface</td>
<td>page 7-262</td>
</tr>
<tr>
<td>username</td>
<td>Configures the names of users accessing this interface</td>
<td>page 7-263</td>
</tr>
</tbody>
</table>
7.1.31.5.1 apn

Configure the access point’s name provided by the service provider. 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>`

Examples

```
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#apn TechPubs
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#

rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#show context
    interface wwan1
        apn TechPubs
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

Related Commands

```
no
```

Removes the configured access point name.
### 7.1.31.5.2 auth-type

**interface-config-wwan-instance**

Configures the authentication types used on this interface

Supported in the following 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>auth-type</th>
<th>Configures the authentication protocol used on this interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>chap</td>
<td>Configures <em>Challenge-Handshake Authentication Protocol</em> (CHAP). This is the default value.</td>
</tr>
<tr>
<td>mschap</td>
<td>Configures <em>Microsoft Challenge-Handshake Authentication Protocol</em> (MSCHAP)</td>
</tr>
<tr>
<td>mschapv2</td>
<td>Configures <em>Microsoft Challenge-Handshake Authentication Protocol</em> (MSCHAP) version 2</td>
</tr>
<tr>
<td>pap</td>
<td>Configures <em>Password Authentication Protocol</em> (PAP)</td>
</tr>
</tbody>
</table>

**Examples**

```bash
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#auth-type mschap-v2
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

```bash
interface wwan1
apn TechPub
    auth-type mschap-v2
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

**Related Commands**

- `no` Removes the authentication protocol configured on this interface
7.1.31.5.3 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>

Examples
rfs4000-229D58 (config-profile-testRFS4000-if-wwan1)#crypto map test
rfs4000-229D58 (config-profile-testRFS4000-if-wwan1)#

rfs4000-229D58 (config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
  apn TechPubs
  auth-type mschap-v2
crypto map test
rfs4000-229D58 (config-profile-testRFS4000-if-wwan1)#

Related Commands
- no
  Removes the crypto map associated with this interface
### 7.1.31.5.4 description

*interface-config-wwan-instance*

Configures a unique description for this interface

**Syntax**

description <WORD>

**Parameters**

- description <WORD>

| description <WORD> | Configures a unique description for this WWAN interface |

**Examples**

```
ap7131-11B6C4(config-device-00-23-68-11-E6-C4-if-wwan1)#description "This interface is reserved for the ISP Airtel"
% Error: Unknown config-item (id:description)
ap7131-11B6C4(config-device-00-23-68-11-E6-C4-if-wwan1)#

rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#description "This interface is reserved for the ISP Airtel"
% Error: Unknown config-item (id:description)
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

**Related Commands**

| no | Removes the description configured for this WWAN interface |
7.1.31.5.5 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

ip [default-gateway|nat]
ip default-gateway priority <1-8000>
ip nat [inside|outside]

Parameters

- ip default-gateway priority <1-8000>
- ip nat [inside|outside]

Examples

rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#ip default-gateway priority 1
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#ip nat inside
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#show context interface wwan1
    apn TechPubs
    auth-type mschap-v2
    crypto map test
    ip nat inside
    ip default-gateway priority 1
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#

Related Commands

no

Removes IP related settings on this interface
7.1.31.5.6 no

```interface-config-wwan-instance```

Removes or reverts the WWAN interface settings

Supported in the following platforms:
- Access Points — AP7131
- Wireless Controllers — RFS4000, RFS6000

**Syntax**

```
no [all|apn|auth-type|crypto|description|ip|password|shutdown|use|username]
```

**Parameters**

None

**Usage Guidelines**

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

**Examples**

```
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#no apn
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#no auth-type
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>apn</strong></td>
<td>Configures the access point’s name provided by the service provider</td>
</tr>
<tr>
<td><strong>auth-type</strong></td>
<td>Configures the authentication types used on this interface</td>
</tr>
<tr>
<td><strong>crypto</strong></td>
<td>Associates a crypto map with this interface</td>
</tr>
<tr>
<td><strong>description</strong></td>
<td>Configures a unique description for this interface</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Configures IP related settings on this interface</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>Configures a password for this WWAN interface</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>Associates an IP ACL with this interface</td>
</tr>
<tr>
<td><strong>username</strong></td>
<td>Configures the names of users accessing this interface</td>
</tr>
</tbody>
</table>
7.1.31.5.7 password

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

```plaintext
password [2 <WORD>|<WORD>]
```

Parameters

- `password [2 <WORD>|<WORD>]`

Examples

```plaintext
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#password TechPubsTesting@123
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

```plaintext
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  ip default-gateway priority 1
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

Related Commands

```plaintext
no
```
7.1.31.5.8 use

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 IP ACL with this interface</td>
</tr>
<tr>
<td>&lt;ACCESS-LIST-NAME&gt;</td>
<td>Specify the IP ACL name.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#use ip-access-list in test
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

```
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
    password TechPubsTesting123
    crypto map test
    ip nat inside
    use ip-access-list in test
    ip default-gateway priority 1
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the IP ACL associated with this interface</td>
</tr>
</tbody>
</table>
7.1.31.5.9 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**

```
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#username TechPubsUser1
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
   username TechPubsUser1
   password TechPubsTesting123
   crypto map test
   ip nat inside
   use ip-access-list in test
   ip default-gateway priority 1
rfs4000-229D58(config-profile-testRFS4000-if-wwan1)#
```

**Related Commands**

```
no
```

Removes the configured username
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-nx4500 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
m1            Select the management interface
port-channel  Select a port channel interface
pppoe1        Select the PPP Over Ethernet interface
radio         Select a radioss
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:

```
authentication            Type of authentication, Eg chap, pap
description               Enter description provided by the service provider
encapsulation             The type of traffic that this group handles.
ip                        Internet Protocol (IP)
local-ip-address          IP address assigned to the local system
no                        Negate a command or set its defaults
password                  Enter password provided by the service provider
remote-ip-subnet          IP subnet assigned to the remote system along with subnet in CIDR notation
remove-override           Remove override from the device
shutdown                  Disable serial interface
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
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#
```
Table 7.19 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 on the serial interface</td>
<td>page 7-266</td>
</tr>
<tr>
<td>description</td>
<td>Configures a description of the serial interface</td>
<td>page 7-267</td>
</tr>
<tr>
<td>encapsulation</td>
<td>Defines the type of traffic handled by the serial interface</td>
<td>page 7-268</td>
</tr>
<tr>
<td>ip</td>
<td>Configures serial interface IP to use NAT</td>
<td>page 7-269</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Assigns a local IP address for this serial interface</td>
<td>page 7-270</td>
</tr>
<tr>
<td>no</td>
<td>Disables or reverts serial interface settings to their defaults</td>
<td>page 7-271</td>
</tr>
<tr>
<td>password</td>
<td>Configures the serial interface’s password</td>
<td>page 7-272</td>
</tr>
<tr>
<td>remote-ip-subnet</td>
<td>Configures the remote system’s IP address and subnet</td>
<td>page 7-273</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides</td>
<td>page 7-274</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the serial interface</td>
<td>page 7-275</td>
</tr>
<tr>
<td>use</td>
<td>Applies an IP access list on this serial interface</td>
<td>page 7-276</td>
</tr>
<tr>
<td>username</td>
<td>Configures the serial interface’s user names</td>
<td>page 7-277</td>
</tr>
</tbody>
</table>
7.1.31.6.1 authentication

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
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#authentication pap

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#show context
interface serial-1/1:1
  authentication pap

nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#

Related Commands

| no | Disables or reverts serial interface settings to their default |
7.1.31.6.2 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
7.1.31.6.3 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 interface serial-1/1:1
  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
7.1.31.6.4 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat</td>
<td>Enables the use of NAT on this serial interface</td>
</tr>
<tr>
<td>inside</td>
<td>Marks this serial interface as NAT inside interface</td>
</tr>
<tr>
<td>outside</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` Enables or reverts serial interface settings to their default
7.1.31.6.5 **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>`

| local-ip-address <IP> | Specify the IP address in the A.B.C.D format |

**Examples**

```text
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
7.1.31.6.6 no

Negates a command or sets its defaults

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax

no <PARAMETER>

Parameters

None

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

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)#

Related Commands

<table>
<thead>
<tr>
<th>Related Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Configures the type of authentication used with this serial interface</td>
</tr>
<tr>
<td>description</td>
<td>Configures the serial interface’s description</td>
</tr>
<tr>
<td>ip</td>
<td>Configures serial interface IP to use NAT</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Assigns a local IP address for this serial interface</td>
</tr>
<tr>
<td>password</td>
<td>Configures the serial interface’s password</td>
</tr>
<tr>
<td>remote-ip-subnet</td>
<td>Configures the remote system’s IP address and subnet</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the serial interface</td>
</tr>
<tr>
<td>use</td>
<td>Applies an IP access list on this serial interface</td>
</tr>
<tr>
<td>username</td>
<td>Configures the names of users accessing this serial interface</td>
</tr>
</tbody>
</table>
### 7.1.31.6.7 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**
```plaintext
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**
- **no** Disables or reverts serial interface settings to their default
7.1.31.6.8 remote-ip-subnet

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 <A.B.C.D/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"
xn4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#

Related Commands
- no
  | Disables or reverts serial interface settings to their default |
7.1.31.6.9 remove-override

Removes device overrides

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

`remove-override <PARAMETERS>`

**Parameters**
None

**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

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)#

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>
7.1.31.6.10 shutdown

Shuts down the serial interface. Use the no shutdown command to re-start a serial interface.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510, NX9600

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>no</td>
<td>Disables or reverts serial interface settings to their default</td>
</tr>
</tbody>
</table>
7.1.31.6.11 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>

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"
nx4500-5CFA2B(config-profile-default-nx45xx-if-serial-1/1:1)#

Related Commands

no
  Disables or reverts serial interface settings to their default
7.1.31.6.12 **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>`

```
username <WORD>          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.
```

**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
7.1.31.7 interface-config-t1e1-instance

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-nx65xx)#interface t1e1 1 1
nx6500-31FABE(config-profile-default-nx65xx-if-t1e1-1/1)#
nx6500-31FABE(config-profile-default-nx65xx-if-t1e1-1/1)#?
```

Table 7.19 summarizes serial 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 7-280</td>
</tr>
<tr>
<td>clock-mode</td>
<td>Configures the selected T1E1 interface’s clock mode</td>
<td>page 7-281</td>
</tr>
<tr>
<td>description</td>
<td>Configures the selected T1E1 interface’s description</td>
<td>page 7-282</td>
</tr>
<tr>
<td>high-impedance</td>
<td>Enables or disables high-impedance monitoring on the selected T1E1 interface</td>
<td>page 7-283</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 7-284</td>
</tr>
<tr>
<td>line-encoding</td>
<td>Configures the selected T1E1 interface’s encoding type</td>
<td>page 7-285</td>
</tr>
<tr>
<td>media</td>
<td>Configures the media type for the physical interface</td>
<td>page 7-286</td>
</tr>
</tbody>
</table>
### Table 7.20 Interface-Config-Serial-Interface Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes or reverts T1E1 interface settings to default</td>
<td>page 7-287</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides on the selected T1E1 interface</td>
<td>page 7-289</td>
</tr>
<tr>
<td>rx-sensitivity-level</td>
<td>Configures the receive sensitivity level in decibels (dB)</td>
<td>page 7-290</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the selected T1E1 interface</td>
<td>page 7-291</td>
</tr>
</tbody>
</table>
7.1.31.7.1 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>
```

**Parameters**

- `channel-group <1-1>`

| channel-group <1-1> | Specify the channel group index |

**Examples**

```
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#channel-group
```

**Related Commands**

| `no` | Removes the channel group configured on the T1E1 interface |
### 7.1.31.7.2 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

```
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#clock-mode normal
```

#### Related Commands

```
no
```
Reverts the T1E1 interface clock mode to default (normal)
7.1.31.7.3 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>

| description <LINE> | Provide a unique description for this T1E1 interface. The description should not exceed 64 characters in length and should help identify the interface. |

Examples

nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)description t1 interface slot 1 NX4524 Main Office

Related Commands

* no

    Removes or resets the T1E1 interface description
7.1.31.7.4 high-impedance

Enables or disables 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]

| high-impedance [disable|enable] | Enables or disables high-impedance |
|--------------------------------|-----------------------------------|
| disable                       | disables high-impedance            |
| enable                        | Enables high-impedance             |

Examples

```
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)high-impedance disable
```

Related Commands

```
no
```
Resets the high impedance setting to either enable or disable.
7.31.7.5 line-build-out

### interface-config-t1e1-instance

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**

```plaintext
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|110-220ft|120OH|15dB|22.5dB|220-330ft|330-440ft|440-550ft|550-660ft|7.5dB|75OH]

| line-build-out [dB|OH|ft] | Defines the line build out in decibels (dB), ohms (OH), or feet (ft) |
|--------------------------|---------------------------------------------------------------------|
| 0-110ft – 0-110 feet (0-33 meters) |
| 0dB – 0 decibels |
| 110-220ft – 110-220 feet (33-67 meters) |
| 120OH – 120 ohms default for E1 |
| 15dB – 15 decibels |
| 22.5dB – 22.5 decibels |
| 220-330ft – 20-330 feet (67-100 meters) |
| 330-440ft – 330-440 feet (100-133 meters) |
| 440-550ft – 440-550 feet (133-167 meters) |
| 550-660ft – 0-110 feet (167-200 meters) |
| 7.5dB – 7.5 decibels |
| 75OH – 75 ohms alternate for E1 |

**Examples**

```
nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-t1e1-1/1)#line-build-out 120OH

nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-t1e1-1/1)#show context
interface t1e1-1/1
 line-build-out 120OH
nx4500-5CFA2B(config-device-B4-C7-99-5C-FA-2B-if-t1e1-1/1)#
```

**Related Commands**

- `no` 
  Resets the T1E1 interface line-build-out setting
### 7.1.31.7.6 line-encoding

**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**

```
nx6500-31FABE(config-profile-default-nx6500-if-t1el-1/1)#line-encoding ami
```

**Related Commands**

- `no`

  Resets the T1E1 interface line-encoding setting
### 7.1.31.7.7 media

**interface-config-t1e1-instance**

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) |

**Examples**

```
rfs7000-37FABE(config-profile-default-nx6500-if-t1e1-1/1)#media t1
```

**Related Commands**

| no | Resets the T1E1 interface media type setting |
### 7.1.31.7.8 no

#### Interface-config-t1e1-instance

Negates or reverts settings to default

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

#### Syntax

```
no <PARAMETER>
```

#### Parameters

None

#### Examples

```
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no ?
channel-group  Channel group for this interface
clock-mode  The mode for the clock
description  Description for this interface
high-impedance  High impedance
line-build-out  Line build out in decibels (dB) or feet (ft)
line-encoding  Line encoding type
media  The media type for the physical interface
no  Negate a command or sets its defaults
remove-override  Remove override from the device
rx-sensitivity-level  Receive sensitivity level in decibels (dB)
shutdown  Disable t1 interface

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
```

```
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no use ip-access-list in
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no allow-management
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no crypto map
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no description
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no dhcp-relay-incoming
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#no ip dhcp client request options all
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)
nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#show context interface vlan8
   ip address 10.0.0.1/8
   ip helper-address 172.16.10.3
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group</td>
<td>Configures the channel group index for this interface</td>
</tr>
<tr>
<td>clock-mode</td>
<td>Configures the mode for the clock on the selected T1E1 interface</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>description</td>
<td>Configures the selected T1E1 interface’s description</td>
</tr>
<tr>
<td>high-impedance</td>
<td>Enables or disables high impedance on the selected T1E1 interface</td>
</tr>
<tr>
<td>line-build-out</td>
<td>Defines the line build out in decibels (dB), ohms (OH), or feet (ft)</td>
</tr>
<tr>
<td>line-encoding</td>
<td>Configures the line encoding type on the selected T1E1 interface</td>
</tr>
<tr>
<td>media</td>
<td>Configures the media type for the physical interface</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides on the selected T1E1 interface</td>
</tr>
<tr>
<td>rx-sensitivity-level</td>
<td>Configures the receive sensitivity level, in decibels (dB), on the selected T1E1 interface</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the selected T1E1 interface</td>
</tr>
</tbody>
</table>
7.1.31.7.9 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**

remove-override <PARAMETERS>

**Parameters**

None

**Examples**

nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#remove-override ?
- channel-group  Channel group for this interface
- clock-mode     The mode for the clock
- description    Description for this interface
- high-impedance High impedance
- line-build-out  Line build out in decibels (dB) or feet (ft)
- line-encoding  Line encoding type
- media          The media type for the physical interface
- no             Negate a command or sets its defaults
- rx-sensitivity-level  Receive sensitivity level in decibels (dB)
- shutdown      Disable t1 interface

nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#

**Related Commands**

\[ no \] Reverts the removal of overrides
7.1.31.7.10 rx-sensitivity-level

    ▶ interface-config-t1e1-instance

Configures 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 <DB>

Parameters

  • rx-sensitivity-level <DB>

<table>
<thead>
<tr>
<th>rx-sensitivity-level &lt;DB&gt;</th>
<th>Sets the receive sensitivity level in decibels (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 0dB – 0 decibels</td>
</tr>
<tr>
<td></td>
<td>• 12dB – 12 decibels</td>
</tr>
<tr>
<td></td>
<td>• 17.5dB – 17.5 decibels</td>
</tr>
<tr>
<td></td>
<td>• 18dB – 18 decibels</td>
</tr>
<tr>
<td></td>
<td>• 22.5dB – 22.5 decibels</td>
</tr>
<tr>
<td></td>
<td>• 30dB – 30 decibels</td>
</tr>
<tr>
<td></td>
<td>• 36dB – 36 decibels</td>
</tr>
<tr>
<td></td>
<td>• 43dB – 43 decibels</td>
</tr>
</tbody>
</table>

Examples

    nx6500-31FABE(config-profile-default-nx6500-if-t1e1-1/1)#rx-sensitivity 36dB

Related Commands

  ▶ no

    Removes or resets rx sensitivity settings
### 7.1.31.7.11 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**

```
nx6500-31FABE(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>Re-starts the T1E1 interface</td>
</tr>
</tbody>
</table>
interface-config-vm-instance

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 sixteen VMIF ports 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)#?
```

VM Interface Mode commands:
- **description** Port description
- **ip** Internet Protocol (IP)
- **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-default-nx45xx-if-vmif2)#
```

```
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  Port description
  ip           Internet Protocol (IP)
  no           Negate a command or set its defaults
  qos          Quality of service
  switchport   Set switching mode characteristics
  use          Set setting to use

  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
  revert       Revert changes
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-nx9000-if-vmif2)#

Table 7.21 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 7-294</td>
</tr>
<tr>
<td>ip</td>
<td>Configures settings related to ARP and DHCP responses</td>
<td>page 7-295</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts the VM interface settings</td>
<td>page 7-296</td>
</tr>
<tr>
<td>qos</td>
<td>Configures the <em>Quality of Service</em> (QoS) settings on this VM interface</td>
<td>page 7-297</td>
</tr>
<tr>
<td>switchport</td>
<td>Defines the switching mode settings for this VM interface</td>
<td>page 7-298</td>
</tr>
<tr>
<td>use</td>
<td>Configures inbound IP and MAC address firewall rules for this VM interface</td>
<td>page 7-300</td>
</tr>
</tbody>
</table>
7.1.31.8.1 description

*interface-config-vm-instance*

Configures a short description of this VM interface

Supported in the following platforms:

- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

description <WORD>

**Parameters**

- description <WORD>

| <WORD> | Provide a short description (64 characters maximum) that uniquely describes this VM interface and differentiates it from others with similar configurations. |

**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)#
```

```
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
7.1.31.8.2 ip

*interface-config-vm-instance*

Configures IP settings related to ARP and DHCP responses

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**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.
7.1.31.8.3 no

- interface-config-vm-instance

Removes or reverts the VM interface settings

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

Syntax
no [description|ip|qos|switchport|use]

Parameters
- no [description|ip|qos|switchport|use]

<table>
<thead>
<tr>
<th>no description</th>
<th>Removes the description configured for this VM interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ip</td>
<td>Removes the ARP and DHCP trust related settings</td>
</tr>
<tr>
<td>no qos</td>
<td>Removes the QoS settings configured for this VM interface</td>
</tr>
<tr>
<td>no switchport</td>
<td>Removes the switching mode settings configured for this VM interface</td>
</tr>
<tr>
<td>no use</td>
<td>Removes the IP or MAC access list associated with this VM interface</td>
</tr>
</tbody>
</table>

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)#
```

```
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#no description
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#no use ip-access-list in
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#no ip arp trust
nx4500-5CFA2B(config-profile-default-nx45xx-if-vmif2)#no ip arp header-mismatch-validation
```

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)#
```
7.1.31.8.4 qos

Configure the Quality of Service (QoS) settings on this VM interface.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

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>
<tbody>
<tr>
<td>trust [802.1p</td>
<td>cos]</td>
</tr>
<tr>
<td>trust dscp</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

Related Commands
- no
  | Removes QoS settings on this VM interface |
7.1.31.8.5 switchport

Defines the switching mode settings for this VM interface.

Supported in the following platforms:
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

```plaintext
switchport [access|mode|trunk]
switchport access vlan <1-4094>
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>]
```

**Parameters**

- `switchport access vlan <1-4094>`
  - Specifies the native VLAN used when the switching mode is set to access. 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 native VLAN.
    - **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 > allowed/native` command to specify the VLANs and the native VLAN.

- `switchport trunk allowed vlan [<1-4094>|add <VLAN-ID>|none|remove <VLAN-ID>]`
  - Specifies the VLANs allowed when the switching mode is set to trunk
  - Creates a list of allowed VLANs (from which packets can be accepted in the trunking mode). This command also allows the modification of an existing list.
    - `<1-4094>` — Configures the list of VLAN IDs
    - `add <VLAN-ID>` — Adds the VLAN ID, identified by the `<VLAN-ID>` 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.
    - `none` — Removes all VLANs from an existing list
    - `remove <VLAN-ID>` — Removes the VLAN ID, identified by the `<VLAN-ID>` keyword, from an existing list
• **switchport trunk native [tagged|vlan <1-4094>]**

<table>
<thead>
<tr>
<th>trunk native</th>
<th>Specifies the native VLAN allowed when the switching mode is set to trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>tagged</td>
<td>Select this option to tag the native VLAN. 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>
</tr>
</tbody>
</table>

| vlan <1-4094> | Select this option for untagged native VLAN. An untagged 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 will be directed over when using trunk mode. The default value is 1. |

**Examples**

```plaintext
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**

| no | Removes the switching mode settings |
7.1.31.8.6 use

Configures inbound IP and MAC address firewall rules for this 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

Syntax
use [ip-access-list|mac-access-list] in <IP/MAC-ACCESS-LIST-NAME>

Parameters
- use [ip-access-list|mac-access-list] in <IP/MAC-ACCESS-LIST-NAME>

<table>
<thead>
<tr>
<th>use ip-access-list in &lt;IP-ACCESS-LIST-NAME&gt;</th>
<th>Applies a IP ACL to the inbound traffic on this VM interface. The IP ACL should be existing and configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>use mac-access-list in &lt;MAC-ACCESS-LIST-NAME&gt;</td>
<td>Applies a MAC ACL to the inbound traffic on this VM interface. The MAC ACL should be existing and configured.</td>
</tr>
</tbody>
</table>

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)#s

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
### 7.1.32 ip

- **Profile Config Commands**

Table 7.22 summarizes NAT pool configuration commands.

**Table 7.22** NAT-Pool-Config-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards etc.</td>
<td>page 7-302</td>
</tr>
<tr>
<td>nat-pool-config-instance</td>
<td>Invokes NAT pool configuration parameters</td>
<td>page 7-308</td>
</tr>
</tbody>
</table>
7.1.32.1  ip

ip

Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards etc.

Supported in the following platforms:

- Access Points — AP300, 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, 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>|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>}
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>
```

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 route <IP/M> <IP>
### Parameters

- **ip default-gateway** `<IP>|failover|priority [dhcp-client <1-1800]|static-route <1-1800>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-gateway</td>
<td>Configures default gateway (next-hop router) parameters</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Configures default gateway’s IP address</td>
</tr>
<tr>
<td>- <code>&lt;IP&gt;</code></td>
<td>Specify the default gateway’s IP address</td>
</tr>
<tr>
<td>failover</td>
<td>Configures failover to the gateway (with next higher priority) when the current default gateway is unreachable (In case of multiple default gateways)</td>
</tr>
<tr>
<td>priority</td>
<td>Configures default gateway priority</td>
</tr>
<tr>
<td>- dhcp-client</td>
<td>Defines a priority for the default gateway acquired by the DHCP client on the VLAN interface</td>
</tr>
<tr>
<td>- static-route</td>
<td>Defines a priority for the statically configured default gateway</td>
</tr>
<tr>
<td>The following keyword is common to 'dhcp-client' and 'static-route' parameters:</td>
<td></td>
</tr>
<tr>
<td>- <code>&lt;1-1800&gt;</code></td>
<td>Specify the priority from 1 - 18000 (lower the value higher is the priority)</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>dns-server-forward</td>
<td>Enables DNS forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network.</td>
</tr>
<tr>
<td>domain-lookup</td>
<td>Enables domain lookup</td>
</tr>
<tr>
<td>domain-name <code>&lt;DOMAIN-NAME&gt;</code></td>
<td>Configures a default domain name</td>
</tr>
<tr>
<td>- <code>&lt;DOMAIN-NAME&gt;</code></td>
<td>Specify a name for the DNS.</td>
</tr>
<tr>
<td>name-server <code>&lt;IP&gt;</code></td>
<td>Configures the name server’s IP address</td>
</tr>
<tr>
<td>- <code>&lt;IP&gt;</code></td>
<td>Specify the IP address of the name server</td>
</tr>
<tr>
<td>routing</td>
<td>Enables IP routing of logically addressed packets from their source to their destination</td>
</tr>
</tbody>
</table>

- **ip dhcp client** `[hostname|persistent-lease]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Configures the DHCP client and host</td>
</tr>
<tr>
<td>client</td>
<td>Sets the DHCP client</td>
</tr>
<tr>
<td>- hostname</td>
<td>Includes the hostname in the DHCP request</td>
</tr>
<tr>
<td>- persistent-lease</td>
<td>Retains the last lease across reboot if the DHCP server is unreachable</td>
</tr>
</tbody>
</table>

- **ip igmp snooping** `{forward-unknown-multicast}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping</td>
<td>Optional. Enables/disables unknown multicast data packets to be flooded in the specified VLAN. By default this feature is disabled.</td>
</tr>
<tr>
<td>forward-unknown-multicast</td>
<td></td>
</tr>
</tbody>
</table>

- **ip igmp snooping querier** `{querier} {max-response-time `<1-25>`|query-interval `<1-18000>`| robustness-variable `<1-7>`|timer expiry `<60-300>`|version `<1-3>`}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping querier</td>
<td>Optional. Enables/disables the IGMP querier functionality for the specified VLAN. By default IGMP snooping querier is disabled.</td>
</tr>
</tbody>
</table>
**max-response-time**<br>**<1-25>**<br>Configures the IGMP maximum query response interval used in IGMP V2/V3 queries for the given VLAN. The default is 10 seconds.

**query-interval**<br>**<1-18000>**<br>Configures the IGMP querier query interval in seconds. Specify a value from 1 - 18000 seconds.

**robustness-variable**<br>**<1-7>**<br>Configures the IGMP robustness variable from 1 - 7

**timer expiry**<br>**<60-300>**<br>Configures the other querier time out value for the given VLAN. The default is 60 seconds.

**version**<br>**<1-3>**<br>Configures the IGMP query version for the given VLAN. The default is 3.
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source static</td>
<td>Specifies source address translation parameters.</td>
</tr>
<tr>
<td>&lt;ACTUAL-IP&gt;</td>
<td>Specify the actual inside IP address to map.</td>
</tr>
<tr>
<td>&lt;1-65535&gt; [tcp</td>
<td>udp]</td>
</tr>
<tr>
<td>&lt;NATTED-IP&gt; &lt;1-65535&gt;</td>
<td>Enables configuration of the outside natted IP address.</td>
</tr>
<tr>
<td>nat</td>
<td>Configures the NAT parameters.</td>
</tr>
<tr>
<td>[inside</td>
<td>outside]</td>
</tr>
<tr>
<td>source list</td>
<td>Configures an access list describing local addresses.</td>
</tr>
<tr>
<td>&lt;IP-ACCESS-LIST-NAME&gt;</td>
<td>Specify a name for the IP access list.</td>
</tr>
<tr>
<td>interface [&lt;INTERFACE-NAME&gt;]</td>
<td>Selects a layer 3 router interface or a VLAN interface.</td>
</tr>
<tr>
<td>pppoe1</td>
<td>vlan &lt;1-4094&gt;</td>
</tr>
<tr>
<td>address &lt;IP&gt;</td>
<td>Configures the interface IP address used with NAT.</td>
</tr>
<tr>
<td>interface &lt;L3-IF-NAME&gt;</td>
<td>Configures a wireless controller or service platform’s VLAN interface.</td>
</tr>
<tr>
<td>overload</td>
<td>Enables use of global address for many local addresses.</td>
</tr>
<tr>
<td>pool &lt;NAT-POOL-NAME&gt;</td>
<td>Specifies the NAT pool.</td>
</tr>
<tr>
<td></td>
<td>Specify the NAT pool name.</td>
</tr>
</tbody>
</table>
- **ip route** `<IP/M>` `<IP>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip route</code></td>
<td>Configures the static routes</td>
</tr>
<tr>
<td><code>&lt;IP/M&gt;</code></td>
<td>Specify the IP destination prefix in the A.B.C.D/M format.</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Specify the IP address of the gateway.</td>
</tr>
</tbody>
</table>

**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
>     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
>     crypto ikev1 remote-vpn
>     crypto ikev2 remote-vpn
>     crypto auto-ipsec-secure
>     interface me1
>     interface ge1
>     ip dhcp trust
>     qos trust dscp
>     qos trust 802.1p
>     interface ge2
>     ip dhcp trust
>     qos trust dscp
>     qos 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 pool1 overload
> ap300 00-15-70-63-4F-86 adopt
> ap300 00-15-70-63-4F-97 adopt
> ap300 00-A0-F8-CF-1E-DA adopt
> 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**

<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>
7.1.32.2 nat-pool-config-instance

Use the config-profile-<DEVICE-PROFILE-NAME> instance to configure Network Address Translation (NAT) pool settings.

<DEVICE>(config-profile-default-<PROFILE-NAME>)#ip nat pool pool1

The following example uses the config-profile-default-rfs7000 instance to configure NAT pool settings:

<DEVICE>(config-profile-default-<PROFILE-NAME>)#ip nat pool pool1

rfs7000-37FABE(config-profile-default-rfs7000)#ip nat pool pool1
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#ip 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)#

Table 7.23 summarizes NAT pool configuration commands.

Table 7.23 NAT-Pool 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 7-309</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 7-310</td>
</tr>
</tbody>
</table>
7.1.32.2.1 address

Configure 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

address [<IP>|range] <START-IP> <END-IP>

Parameters
- address [<IP>|range <START-IP> <END-IP>]

<table>
<thead>
<tr>
<th>address &lt;ip&gt;</th>
<th>Adds a single IP address to the NAT pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>range &lt;START-IP&gt; &lt;END-IP&gt;</td>
<td>Adds a range of IP addresses to the NAT pool</td>
</tr>
<tr>
<td>&lt;START-IP&gt; – Specify the starting IP address of the range.</td>
<td></td>
</tr>
<tr>
<td>&lt;END-IP&gt; – Specify the ending IP address of the range.</td>
<td></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 |
7.1.32.2.2 no

Removes address(es) configured with this NAT pool

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
no address

Parameters
None

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) |
### 7.1.33 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6523, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|manual-session|router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port <1024-65535>]
```

#### Parameters

- **hostname `<HOSTNAME>`** — Configures the L2TPv3 specific host name.
- **inter-tunnel-bridging** — Enables inter tunnel bridging of packets. This feature is disabled by default.
- **manual-session** — Creates/modifies L2TPv3 manual sessions
  For more information, see [l2tpv3-manual-session-commands](#).
- **router-id `<1-4294967295>|<IP>`** — Configures the router ID sent in the L2TPv3 signalling messages
  - `<1-4294967295>` — Configures the router ID in decimal format from 1 - 4294967295
  - `<IP>` — Configures the router ID in the IP address (A.B.C.D) format
- **tunnel** — Creates/modifies a L2TPv3 tunnel
  For more information, see [l2tpv3-tunnel-commands](#).
- **udp-listen-port `<1024-65535>`** — Configures the UDP port used to listen for incoming traffic
  - `<1024-65535>` — Specify the UDP port from 1024 - 65535 (default is 1701)
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 |
7.1.34 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:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

l3e-lite-table aging-time <10-1000000>

Parameters

- l3e-lite-table aging-time <10-1000000>

Example

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
7.1.35 led

Profile Config Commands

Turns on and off access point LEDs

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

led {flash-pattern}

Parameters

- led {flash-pattern}

flash-pattern Optional. Enables LED flashing on the device using this profile

Select this option to flash an access point’s LEDs in a distinct manner (different from its operational LED behavior). Enabling this feature allows an administrator to validate an access point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.

Examples

rfs7000-37FABE(config-profile-RFS7000Test)#led flash-pattern
rfs7000-37FABE(config-profile-RFS7000Test)#

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
### 7.1.36 led-timeout

**Profile Config Commands**

Configures the LED-timeout timer in the device or profile configuration mode.

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

**Syntax**

`led-timeout [<15-1440>|shutdown]`

**Parameters**

- `led-timeout [<15-1440>|shutdown]`

**Examples**

```plaintext
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
66069c24b3bb1259eb36826cab3cc83999d408f0ff891e74b62b2d3594f0b3ddee7967f30e49e497
license HTANLT
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
66069c24b3bb1259eb36826cab3cc83999d408f0ff891e74b62b2d3594f0b3ddee7967f30e49e497
license HTANLT
no autogen-uniqueid
ip default-gateway 192.168.13.2
led-timeout shutdown
crypto ikev2 peer IKEv2Peer1
--More--
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

**Related Commands**

- `no` | Disables LED-timeout timer
7.1.37 legacy-auto-downgrade

Profile Config Commands

Enables device firmware to auto downgrade when legacy devices are detected.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
legacy-auto-downgrade
```

Parameters

None

Examples

```plaintext
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><code>no</code></td>
<td>Prevents device firmware from auto downgrading when legacy devices are detected</td>
</tr>
</tbody>
</table>
### 7.1.38 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>legacy-auto-update</td>
<td>Updates a legacy AP650 or AP7131 access point firmware</td>
</tr>
<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>image</td>
<td>Sets the path to the firmware image</td>
</tr>
<tr>
<td>&lt;FILE&gt;</td>
<td>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
## 7.1.39 lldp

### Profile Config Commands

Configures LLDP settings

Supported in the following platforms:

- **Access Points** — AP300, 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, 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]
```

### Parameters

- **holdtime <10-1800>|run|timer <5-900>**
  - Sets the holdtime for transmitted LLDP PDUs. This command specifies the time a receiving device holds information before discarding it.
  - **<10-1800>** – Specify a holdtime from 10 - 1800 seconds.
  - **run** – Enables LLDP
  - **timer <5-900>** – Specify transmit interval from 5 - 900 seconds.

- **lldp med-tlv-select [inventory-management|power-management]**
  - Provides additional media endpoint device TLVs to enable inventory and power management discovery. Specifies the LLDP MED TLVs to send or receive.
  - **inventory-management** – Enables inventory management discovery. Allows an endpoint to convey detailed inventory information about itself.
  - **power-management** – Enables extended power via MDI discovery. Allows endpoints to convey power information, such as how the device is powered, power priority etc.

### 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
                      .........................
  ip nat pool pooll
  address range 172.16.10.2 172.16.10.8
  ip nat inside source list test interface vlan1 pool pooll overload
  lldp timer 20
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

### Related Commands

- **no**  
  Disables LLDP on this profile
### 7.1.40 load-balancing

**Profile Config Commands**

Configures load balancing parameters

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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|ap-load] [client-weightage|throughput-weightage] <0-100>`

- `load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <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 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|use-wips]`

**Parameters**

- `load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load] [client-weightage|throughput-weightage] <0-100>`

<table>
<thead>
<tr>
<th>advanced-params</th>
<th>Configures advanced load balancing parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz-load</td>
<td>Configures 2.4 GHz load calculation weightages</td>
</tr>
<tr>
<td>[client-weightage</td>
<td>throughput-weightage]</td>
</tr>
<tr>
<td></td>
<td>- throughput-weightage – Specifies weightage assigned to throughput, when calculating the 2.4 GHz band, channel, or radio 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</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5GHz-load</td>
<td>Configures 5.0 GHz load calculation weightages</td>
</tr>
<tr>
<td>[client-weightage]</td>
<td>• client-weightage – Specifies weightage assigned to the client-count when calculating the 5.0 GHz load</td>
</tr>
<tr>
<td>[throughput-weightage]</td>
<td>• throughput-weightage – Specifies weightage assigned to throughput, when calculating the 5.0 GHz band, channel or radio load</td>
</tr>
<tr>
<td>&lt;0-100&gt;</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</td>
</tr>
<tr>
<td>ap-load</td>
<td>Configures AP load calculation weightages</td>
</tr>
<tr>
<td>[client-weightage]</td>
<td>• client-weightage – Specifies weightage assigned to the client-count, when calculating the AP load</td>
</tr>
<tr>
<td>[throughput-weightage]</td>
<td>• throughput-weightage – Specifies weightage assigned to throughput, when calculating the AP load</td>
</tr>
<tr>
<td>&lt;0-100&gt;</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</td>
</tr>
</tbody>
</table>

- `load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <0-100>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced-params</td>
<td>Configures advanced load balancing parameters</td>
</tr>
<tr>
<td>equality-margin</td>
<td>Configures the maximum load difference considered equal. The load is compared for different 2.4 GHz channels, 5.0 GHz channels, AP, or bands.</td>
</tr>
<tr>
<td>[2.4GHz</td>
<td>5GHz</td>
</tr>
<tr>
<td>&lt;0-100&gt;</td>
<td>• 5GHz – Configures the maximum load difference considered equal when comparing loads on different 5.0 GHz channels</td>
</tr>
<tr>
<td></td>
<td>• ap – Configures the maximum load difference considered equal when comparing loads on different APs</td>
</tr>
<tr>
<td></td>
<td>• band – Configures the maximum load difference considered equal when comparing loads on different bands</td>
</tr>
<tr>
<td></td>
<td>The following keyword is common to 2.4 GHz channels, 5.0 GHz channels, APs, and bands:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-100&gt; – Sets the margin as a load percentage from 1 - 100</td>
</tr>
</tbody>
</table>

- `load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|channel-5GHz] <0-100>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced-params</td>
<td>Configures advanced load balancing parameters</td>
</tr>
<tr>
<td>hiwater-threshold</td>
<td>Configures the load beyond which load balancing is invoked</td>
</tr>
<tr>
<td><strong>Profiles 7 - 321</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td></td>
</tr>
</tbody>
</table>

- **load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHz] <0-100>**

<table>
<thead>
<tr>
<th><strong>advanced-params</strong></th>
<th>Configures advanced load balancing parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>max-preferred-band-load</strong></td>
<td>Configures the maximum load on the preferred band, beyond which the other band is equally preferred</td>
</tr>
</tbody>
</table>

- **[2.4GHz|5GHz] <0-100>**

<table>
<thead>
<tr>
<th><strong>Select one of the following options:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2.4GHz – Configures the maximum load on 2.4 GHz, when it is the preferred band</td>
</tr>
<tr>
<td>• 5GHz – Configures the maximum load on 5.0 GHz, when it is the preferred band</td>
</tr>
</tbody>
</table>

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

- **load-balancing advanced-params [max-neighbors <0-16>|min-common-clients <0-256>|min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]**

<table>
<thead>
<tr>
<th><strong>advanced-params</strong></th>
<th>Configures advanced load balancing parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>max-neighbors &lt;0-6&gt;</strong></td>
<td>Configures the maximum number of confirmed neighbors to balance</td>
</tr>
<tr>
<td>• &lt;0-6&gt; – Specify a value from 0 - 6. Optionally configure a minimum of 0 neighbors and a maximum of 6 neighbors</td>
<td></td>
</tr>
<tr>
<td><strong>min-common-clients &lt;0-256&gt;</strong></td>
<td>Configures the minimum number of common clients that can be shared with the neighbor for load balancing</td>
</tr>
<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.</td>
<td></td>
</tr>
<tr>
<td><strong>min-neighbor-rssi &lt;100-30&gt;</strong></td>
<td>Configures the minimum signal strength (Received Signal Strength Indicator - RSSI) of a neighbor detected</td>
</tr>
<tr>
<td>• &lt;100-30&gt; – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm.</td>
<td></td>
</tr>
<tr>
<td><strong>min-probe-rssi &lt;100-30&gt;</strong></td>
<td>Configures the minimum received probe signal strength required to qualify the sender as a common client</td>
</tr>
<tr>
<td>• &lt;0-100&gt; – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm.</td>
<td></td>
</tr>
</tbody>
</table>

- **load-balancing balance-ap-loads [2.4GHz|5GHz]**

<p>| <strong>balance-ap-loads</strong> | Enables neighbor AP load balancing. This option distributes the access point's radio load amongst other controller managed access point radios. This option is enabled by default. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 enabled 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  
  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  
  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. |
| band-control-strategy         | Configures a band control strategy                                                                                                                                                                           |
| distribute-by-ratio           | Distributes clients to either band according to the band-ratio                                                                                                                                                 |
| prefer-2.4GHz                 | Nudges all dual-band clients to 2.4 GHz band                                                                                                                                                                   |
| prefer-5GHz                   | Nudges all dual-band clients to 5.0 GHz band                                                                                                                                                                   |
| band-ratio [2.4GHz 5GHz]      | 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 1.                                                                                                             |
| 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.                                                                                                             |
| group-id <GROUP-ID>           | Configures group ID to facilitate load balancing  
  • <GROUP-ID> – Specify the group ID.                                                                                                                |
| 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                                                                                                                                             |
| use-roam-notification          | Selects neighbors based on roam notifications from roamed clients                                                                                                                                                |
| use-smart-rf                  | Selects neighbors detected by Smart RF                                                                                                                                                                           |
Examples

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--

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables load balancing on this profile</td>
</tr>
</tbody>
</table>
### 7.1.41 logging

**Profile Config Commands**

Enables message logging and configures logging settings. This command can also be executed in the device configuration mode.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
logging [aggregation-time|buffered|console|facility|forward|host|on|syslog]
```

```
logging [aggregation-time <1-60>|host <IP>|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**

- **aggregation-time <1-60>** — Sets the number of seconds for aggregating repeated messages
  - `<1-60>` – Specify a value from 1 - 60 seconds.

- **host <IP>** — Configures a remote host to receive log messages. Defines numerical (non DNS) IP addresses for external resources where logged system events can be sent on behalf of the controller profile.
  - `<IP>` – Specify the IP 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]**

- **buffered** — Sets the buffered logging level
- **console** — Sets the console logging level
- **syslog** — Sets the syslog server’s logging level
- **forward** — Forwards system debug messages to the wireless controller or service platform
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.

- `<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 (default)
- `notifications` – Severity level 5: Normal but significant conditions
- `informational` – Severity level 6: Informational messages
- `debugging` – Severity level 7: Debugging messages

| facility [local0|local1|local2|local3|local4|local5|local6|local7] | Enables the syslog to decide where to send the incoming message. There are 8 logging facilities, from syslog0 to syslog7. |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| local0 – Syslog facility local0                  | local0 – Syslog facility local0                                                                                 |
| local1 – Syslog facility local1                  | local1 – Syslog facility local1                                                                                 |
| local2 – Syslog facility local2                  | local2 – Syslog facility local2                                                                                 |
| local3 – Syslog facility local3                  | local3 – Syslog facility local3                                                                                 |
| local4 – Syslog facility local4                  | local4 – Syslog facility local4                                                                                 |
| local5 – Syslog facility local5                  | local5 – Syslog facility local5                                                                                 |
| local6 – Syslog facility local6                  | local6 – Syslog facility local6                                                                                 |
| local7 – Syslog facility local7                  | local7 – Syslog facility local7                                                                                 |

**Examples**

```
  rfs7000-37FABE(config-profile-default-rfs7000)#logging facility local4

  rfs7000-37FABE(config-profile-default-rfs7000)#show context profile rfs7000 default-rfs7000
  bridge vlan 1
  ...................................................
  ip dns-server-forward
  **logging facility local4**
  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
  ap300 00-15-70-63-4F-86 adopt
  ap300 00-15-70-63-4F-97 adopt
  ap300 00-A0-F8-CF-1E-DA adopt
  service pm sys-restart
  router ospf
  l2tpv3 hostname l2tpv3Host1
  l2tpv3 inter-tunnel-bridging
  rfs7000-37FABE(config-profile-default-rfs7000)#
```

**Related Commands**

- `no` Disables logging on this profile
7.1.42 mac-address-table

Profile Config Commands

Configures the MAC address table. Use this command to assign a static address to the MAC address table.

Supported in the following platforms:
- Access Points — AP300, 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, 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>]
  - 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 -100000 seconds
- mac-address-table static <MAC> vlan <1-4094> interface [<<L2-INTERFACE>|ge <1-4>| 
  port-channel <1-2>]
  - static <MAC>
    - Creates a static MAC address table entry
      - <MAC> – Specifies the static address to add to the MAC address table. Specify the MAC
  - 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 ge1
  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>
7.1.43 mac-auth

Profile Config Commands

Enables or disables authentication of a client’s MAC address on wired ports. When configured, MAC authentication will be enabled on devices using this profile.

To enable MAC address authentication on a device, enter the device’s configuration mode and execute the `mac-auth` command.

When enabled, the source MAC address of a device, connected to the specified wired port, is authenticated with the RADIUS server. Once authenticated the device is permitted access to the managed network and packets from the authenticated source are processed. If not authenticated the device is either denied access or provided guest access through the guest VLAN (provided guest VLAN access is configured on the port).

Enabling MAC authentication requires you to first configure a AAA policy specifying the RADIUS server. Configure the client’s MAC address on the specified RADIUS server. Attach this AAA policy to a profile or a device. Finally, enable MAC authentication on the desired wired port of the device or device-profile.

Only one MAC address is supported for every wired port. Consequently, when one source MAC address is authenticated, packets from all other sources are dropped.

To enable client MAC authentication on a wired port:

1. Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.
   a. `<DEVICE>(config)#radius-group <RAD-GROUP-NAME>`
   `<DEVICE>(config-radius-group-<RAD-GROUP-NAME>)#policy vlan <VLAN-ID>`
   b. `<DEVICE>(config)#radius-user-pool-policy <RAD-USER-POOL-NAME>`
   `<DEVICE>(config-radius-user-pool-<RAD-USER-POOL-NAME>)#user <USER-NAME> password <PASSWORD> group <RAD-GROUP-OF-STEP-A>`
   Note: The `<USER-NAME>` and `<PASSWORD>` should be the client’s MAC address. This address will be matched against the MAC address of incoming traffic at the specified wired port.
   c. `<DEVICE>(config)#radius-server-policy <RAD-SERVER-POL-NAME>`
   `<DEVICE>(config-radius-server-policy-<RAD-SERVER-POL-NAME>)#use radius-user-pool-policy <RAD-USER-POOL-OF-STEP-B>`

2. Configure a AAA policy exclusively for wired MAC authentication and specify the authentication (RADIUS) server settings. The following example creates a AAA policy ‘macauth’ and enters its configuration mode:
   `<DEVICE-A>(config)#aaa-policy macauth
   <DEVICE-A>(config-aaa-policy-macauth)#...`
   Specify the RADIUS server details.
   `<DEVICE-A>(config)#aaa-policy macauth
   <DEVICE-A>(config-aaa-policy-macauth)#authentication server <1-6> [host <IP>|onboard]`
   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.
   `<DEVICE>(config-device-aa-bb-cc-dd-ee)#mac-auth use aaa-policy macauth
   <DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#mac-auth use aaa-policy macauth`

3. 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.
   `<DEVICE>(config-device-aa-bb-cc-dd-ee)#interface ge x
   <DEVICE>(config-device-aa-bb-cc-dd-ee-gex)#mac-auth
   <DEVICE>(config-profile-<PROFILE-NAME>)#interface ge x
   <DEVICE>(config-profile-<PROFILE-NAME>)#mac-auth`
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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac-auth</code></td>
<td>Enables 802.1X authentication of MAC addresses on this profile. Use the device configuration mode to enable this feature on a device.</td>
</tr>
<tr>
<td><code>use aaa-policy &lt;AAA-POLICY-NAME&gt;</code></td>
<td>Associates an existing AAA policy with this profile (or device)</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;AAA-POLICY NAME&gt;</code> – Specify the AAA policy name.</td>
</tr>
<tr>
<td></td>
<td>The AAA policy used should be created especially for MAC authentication.</td>
</tr>
</tbody>
</table>

**Examples**

The following examples demonstrate the configuration of authentication of MAC addresses on wired ports:

```bash
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
    authentication server 1 onboard controller
rfs4000-229D58(config-aaa-policy-mac-auth)#

rfs4000-229D58(config)#radius-group RG
rfs4000-229D58(config-radius-group-RG)#policy vlan 11

rfs4000-229D58(config-radius-group-RG)#show context
  radius-group RF
    policy vlan 11
rfs4000-229D58(config-radius-group-RG)#

rfs4000-229D58(config)#radius-user-pool-policy RUG
rfs4000-229D58(config-radius-user-pool-RUG)#user 00-16-41-55-F8-5D password 0 00-16-41-55-F8-5D group RG

rfs4000-229D58(config-radius-user-pool-RUG)#show context
  radius-user-pool-policy RUG
    user 00-16-41-55-F8-5D password 0 00-16-41-55-F8-5D group RG
rfs4000-229D58(config-radius-user-pool-RUG)#

rfs4000-229D58(config)#radius-server-policy RS
rfs4000-229D58(config-radius-server-policy-RS)#use radius-user-pool-policy RUG

rfs4000-229D58(config-radius-server-policy-RS)#show context
  radius-server-policy RS
    use 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

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#
```
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**

| **no** | Disables authentication of MAC addresses on wired ports settings on this profile (or device) |
7.1.44 memory-profile

Profile Config Commands

Configures memory profile used on the device

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

memory-profile [adopted|standalone]

Parameters

- memory-profile [adopted|standalone]

<table>
<thead>
<tr>
<th>adopted</th>
<th>Configures adopted mode (no GUI and higher MiNT routes, firewall flows)</th>
</tr>
</thead>
<tbody>
<tr>
<td>standalone</td>
<td>Configures standalone mode (GUI and fewer MiNT routes, firewall flows)</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#memory-profile adopted
% Error on default-rfs7000: memory-profile is not supported on this device
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

- no resets device’s memory profile configuration
### 7.1.45 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 — AP71XX

#### Syntax

```
meshpoint-device <MESHPOINT-NAME>
```

#### Parameters

- `meshpoint-device <MESHPOINT-NAME>`

| meshpoint-device <MESHPOINT-NAME> | Configures meshpoint device parameters
|-----------------------------------|-----------------------------------------------|
|                                  | • `<MESHPOINT-NAME>` – Specify meshpoint name.

#### 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

```
rfs7000-37FABE(config-profile-testAP71XX)#meshpoint-device test
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
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-testAP71XX-meshpoint-test)#
```

#### Related Commands

| no  | Removes a specified meshpoint |

#### NOTE:

For more information on the meshpoint-device configuration parameters, see *Chapter 27, MESHPOINT*, section MESHPOINT.
7.1.46 meshpoint-monitor-interval

Profile Config Commands

Configures the meshpoint monitoring interval. This is the interval, in seconds, the up/down status of a meshpoint is checked. Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

`meshpoint-monitor-interval <1-65535>`

Parameters

- meshpoint-monitor-interval <1-65535>

Examples

```bash
rfs7000-37FABE(config-profile-default-rfs7000)#meshpoint-monitor-interval 100
```

```bash
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--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

Related Commands

- `no` — Resets the meshpoint monitoring interval to default (30 seconds)
7.1.47 min-misconfiguration-recovery-time

Profile Config Commands

Configures the minimum device connectivity verification time.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

min-misconfiguration-recovery-time <60-3600>

Parameters

- min-misconfiguration-recovery-time <60-3600>

<table>
<thead>
<tr>
<th>min-misconfiguration-recovery-time &lt;60-3600&gt;</th>
<th>Configures the minimum connectivity (with the associated device) verification interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;60-3600&gt; — Specify a value from 1 - 3600 seconds (default is 60 seconds).</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37PABE(config-profile-default-rfs7000)#min-misconfiguration-recovery-time 200
% Error on default-rfs7000: Unknown config-item (id:min_misconf_recovery_time)
rfs7000-37PABE(config-profile-default-rfs7000)#

Related Commands

no

Resets setting to default (60 seconds)
7.1.48 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

mint [dis|level|link|mlcp|rate-limit|spf-latency|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 force ip [<IPv4>|<IPv6>] [level 2|level 2] {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-secure {gw [<IP>|<HOST-NAME>]}}


mint link ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>] {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]


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-controller-load-balancing level1

Parameters

- mint dis [priority-adjustment <-255-255>|strict-evis-reachability]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dis priority-adjustment &lt;-255-255&gt;</td>
<td>Sets the relative priority for the router to become DIS (designated router)</td>
</tr>
<tr>
<td>priority-adjustment</td>
<td>Sets priority adjustment added to base priority</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>&lt;255-255&gt;</td>
<td>Specify a value from 255-255. The default is 0.</td>
</tr>
<tr>
<td>strict-evis-reachability</td>
<td>Enables reaching EVIS election winners through MiNT</td>
</tr>
</tbody>
</table>

Note: Higher numbers result in higher priorities.
### mint level 1 area-id <1-16777215>

**level 1**
- Configures local MiNT routing settings
  - **1** – Configures local MiNT routing level

**area-id <1-16777215>**
- Specifies the level 1 routing area identifier
  - **<1-16777215>** – Specify a value from 1 - 16777215.

### mint link force ip [IPv4|IPv6] [level 2] {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120}|ipsec-security {gw [IP|HOST-NAME]}}

**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.
  - **level** – Specifies the routing level
  - **2** – Configures level 2 inter-site MiNT routing

**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 <1-100000>**
- Optional. Specifies the link cost in arbitrary units
  - **<1-100000>** – 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 seconds. The default is 15 seconds.

**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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **link 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>** | Enables MINT routing on 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>** | 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>** | 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]** | 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>}** | 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. |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| link ip [IPv4|IPv6] <HOST-ALIAS-NAME> | Creates a MiNT routing link  
- ip – Creates a MiNT tunnel over UDP/IP 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 IPv4 address used by peers.  
- <IPv6> – Specify the IPv6 address used by peers.  
- <HOST-ALIAS-NAME> – Specify the host alias identifying the MiNT tunnel peer’s address. The host alias should existing and configured. |
| <1-65535>    | Select 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 <1-100000> | Optional. Specifies the link cost in arbitrary units  
- <1-100000> – 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]**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| mlcp [ip|ipv6]vlan | Configures the MiNT Link Creation Protocol (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 IPv6 address.  
- ipv6 – Enables MLCP over layer 3 (UDP/IP6) links |
- **mint rate-limit level2**
  mlcp [ip|ipv6|vlan] rate <50-1000000> max-burst-size <2-1024> {red-threshold [background|best-effort|video|voice] <0-100>}

**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/IP
- ipv6 – Configures rate-limits for MLCP over UDP/IPv6 links
- vlan – Configures rate-limiting 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.
### mint spf-latency <0-60>

Specifies the latency of SPF routing recalculation. This option allows you to set the latency of routing recalculation option (within the Shortest Path First (SPF) field). This option is disabled by default.

- `<0-60>` — Specify the latency from 0 - 60 seconds.

### 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

```bash
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 1
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
--More--
rfs7000-37FABE(config-profile-default-rfs7000)#
```

### Related Commands

- **no** — Disables or reverts settings to their default.
7.1.49 misconfiguration-recovery-time

Profile Config Commands

Verifies connectivity after a configuration is received

Supported in the following platforms:

- Access Points — AP300, 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, 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>
<tbody>
<tr>
<td>0</td>
<td>Disables recovery from misconfiguration</td>
</tr>
</tbody>
</table>

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
  ap300 00-15-70-63-4F-86 adopt
  ap300 00-15-70-63-4F-97 adopt
  ap300 00-A0-F8-CF-1E-DA adopt
  service pm sys-restart
  router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

no Reverts to default (180 seconds)
7.1.50 neighbor-inactivity-timeout

Profile Config Commands

Configures neighbor inactivity timeout

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

neighbor-inactivity-timeout <1-1000>

Parameters

- neighbor-inactivity-timeout <1-1000>

<table>
<thead>
<tr>
<th>&lt;1-1000&gt;</th>
<th>Sets neighbor inactivity timeout</th>
</tr>
</thead>
</table>
| <1-1000> | Specify a value from 1 - 1000 seconds.

Examples

rfs7000-37FABE(config-profile-default)#neighbor-inactivity-timeout 500

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-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
  qos trust 802.1p
--More--

rfs7000-37FABE(config-profile-default-rfs7000)#
### 7.1.51 neighbor-info-interval

**Profile Config Commands**

Configures the neighbor information exchange interval

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

neighbor-info-interval <1-100>

**Parameters**

- neighbor-info-interval <1-100>

| <1-100> | Sets interval in seconds from 1 - 100 |

**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)#
```
7.1.52 no

Profile Config Commands

Negates a command or resets values to their default

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax


Parameters

None

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)#no cluster

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</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>
</tr>
<tr>
<td>adoption</td>
<td>Configures adoption time delay settings</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, VLAN, and service aliases on this profile</td>
</tr>
<tr>
<td>ap300</td>
<td>Enables adoption of AP300s</td>
</tr>
<tr>
<td>area</td>
<td>Sets the area name where the system is located</td>
</tr>
<tr>
<td>arp</td>
<td>Configures static address resolution protocol</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enables network configuration device learning</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>
</tr>
<tr>
<td>autoinstall</td>
<td>Configures the autoinstall feature</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures bridge specific commands</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures captive portal advanced Web page uploads on a profile or device</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cdp</td>
<td>Enables CDP on a device</td>
</tr>
<tr>
<td>cluster</td>
<td>Configures a cluster name</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enables configuration persistence across reloads</td>
</tr>
<tr>
<td>controller</td>
<td>Configures a wireless controller or service platform</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Monitors user configured IP addresses and logs their status</td>
</tr>
<tr>
<td>crypto</td>
<td>Configures crypto settings</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings on this profile</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures 802.1x standard authentication controls</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configures an IP DSCP to 802.1p priority mapping for untagged frames</td>
</tr>
<tr>
<td>email-notification</td>
<td>Configures e-mail notification</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Enables checking of a device’s firmware version before attempting adoption or clustering</td>
</tr>
<tr>
<td>environmental-sensor</td>
<td>Configures the environmental sensor device settings</td>
</tr>
<tr>
<td>events</td>
<td>Displays system event messages</td>
</tr>
<tr>
<td>export</td>
<td>Enables the export of the startup.log file after every boot</td>
</tr>
<tr>
<td>floor</td>
<td>Sets the floor name where the system is located</td>
</tr>
<tr>
<td>gre</td>
<td>Enables GRE tunneling on this device</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Configures HTTP analysis settings</td>
</tr>
<tr>
<td>interface</td>
<td>Configures an interface</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP components</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Defines the Layer 2 Tunnel Protocol (L2TP) protocol for tunneling layer 2 payloads using VPNs</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>Configures L3e Lite Table with this profile</td>
</tr>
<tr>
<td>led</td>
<td>Turns device LEDs on or off</td>
</tr>
<tr>
<td>led-timeout</td>
<td>Configures LED-timeout timer. This command is specific to the NX9000 series service platforms.</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Auto downgrades a legacy device firmware</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto upgrades a legacy device firmware</td>
</tr>
<tr>
<td>lldp</td>
<td>Configures Link Layer Discovery Protocol (LLDP)</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configures load balancing parameters</td>
</tr>
<tr>
<td>logging</td>
<td>Modifies message logging</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Configures the MAC address table</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables 802.1x port-based user authentication on this device</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Configures the memory profile used on the device</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configures the meshpoint device parameters</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configures the meshpoint monitoring interval</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Configures the minimum connectivity (with connected device) verification time</td>
</tr>
<tr>
<td>mint</td>
<td>Configures the MiNT protocol settings</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Verifies connectivity after a device configuration file is received</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configures neighbor inactivity timeout</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configures the neighbor information exchange interval</td>
</tr>
<tr>
<td>noc</td>
<td>Configures NOC settings</td>
</tr>
<tr>
<td>ntp</td>
<td>Configures an NTP server</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>
</tr>
<tr>
<td>power-config</td>
<td>Configures the power option mode. Sets the amount of power that the access point draws.</td>
</tr>
<tr>
<td>preferred-controller-group</td>
<td>Specifies the wireless controller or service platform’s group preferred for adoption</td>
</tr>
<tr>
<td>preferred-tunnel-controller</td>
<td>Configures the tunnel wireless controller or service platform’s name preferred for tunneling extended VLAN traffic</td>
</tr>
<tr>
<td>radius</td>
<td>Configures device-level RADIUS authentication parameters</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Enables RF Domain manager</td>
</tr>
<tr>
<td>router</td>
<td>Configures dynamic router protocol settings</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Enables automatic AP firmware upgrade</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Configures the tunneled WLAN (extended-VLAN) wireless controller’s name</td>
</tr>
<tr>
<td>use</td>
<td>Defines the settings used by this feature</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configures VRRP group settings</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enables support for 802.11 WEP shared key authentication</td>
</tr>
</tbody>
</table>
7.1.53 noc

Profile Config Commands

Configures Network Operations Center (NOC) settings, such as NOC statistics update interval

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

noc update-interval [<5-3600>|auto]

Parameters

- noc update-interval [<5-3600>|auto]

<table>
<thead>
<tr>
<th>update-interval</th>
<th>Configures NOC statistics update interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>[&lt;5-3600&gt;</td>
<td>auto]</td>
</tr>
<tr>
<td></td>
<td>• auto – The NOC statistics update interval is automatically adjusted by the wireless controller or service platform based on load</td>
</tr>
</tbody>
</table>

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
bridge-isolated-tunnel
ip igmp snooping
ip igmp snooping querier
interface pppoe1
use firewall-policy default
misconfiguration-recovery-time 65
noc update-interval 25
ap300 00-15-70-63-4F-86 adopt
ap300 00-15-70-63-4F-97 adopt
ap300 00-A0-F8-CF-1E-DA adopt
service pm sys-restart
router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

no

Resets NOC related parameters
### 7.1.54 ntp

Profile Config Commands

Configures the Network Time Protocol (NTP) server settings

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp server <code>&lt;PEER-IP&gt;</code> {autokey</td>
<td>key</td>
</tr>
<tr>
<td>ntp server <code>&lt;PEER-IP&gt;</code> {autokey} {prefer version <code>&lt;1-4&gt;</code></td>
<td>version <code>&lt;1-4&gt;</code>}</td>
</tr>
<tr>
<td>ntp server <code>&lt;PEER-IP&gt;</code> {key <code>&lt;1-65534&gt;</code> md5 [0 &lt;WORD&gt;</td>
<td>2&lt;WORD&gt;</td>
</tr>
<tr>
<td>ntp server <code>&lt;PEER-IP&gt;</code> {prefer version <code>&lt;1-4&gt;</code></td>
<td>version <code>&lt;1-4&gt;</code> prefer}</td>
</tr>
</tbody>
</table>

Parameters

- ntp server `<PEER-IP>` {autokey} {prefer version `<1-4>`|version `<1-4>`}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server <code>&lt;PEER-IP&gt;</code></td>
<td>Configures a NTP server association</td>
</tr>
<tr>
<td>autokey {prefer version <code>&lt;1-4&gt;</code></td>
<td>version <code>&lt;1-4&gt;</code>}</td>
</tr>
<tr>
<td>version <code>&lt;1-4&gt;</code></td>
<td>Select the NTP version</td>
</tr>
<tr>
<td>prefer</td>
<td>Optional. Prefers this peer when possible</td>
</tr>
<tr>
<td>version <code>&lt;1-4&gt;</code></td>
<td>Select the NTP version</td>
</tr>
<tr>
<td>ntp server <code>&lt;IP&gt;</code> {key <code>&lt;1-65534&gt;</code> md5 [0 &lt;WORD&gt;</td>
<td>2&lt;WORD&gt;</td>
</tr>
<tr>
<td>key <code>&lt;1-65534&gt;</code> md5 [0 &lt;WORD&gt;</td>
<td>2&lt;WORD&gt;</td>
</tr>
<tr>
<td>0 &lt;WORD&gt;</td>
<td>Configures a clear text password</td>
</tr>
<tr>
<td>2 &lt;WORD&gt;</td>
<td>Configures an encrypted password</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>Sets an authentication key</td>
</tr>
<tr>
<td>prefer version <code>&lt;1-4&gt;</code></td>
<td>Optional. Prefers this peer when possible</td>
</tr>
<tr>
<td>version <code>&lt;1-4&gt;</code></td>
<td>Select the NTP version</td>
</tr>
<tr>
<td>prefer {version <code>&lt;1-4&gt;</code>}</td>
<td>Optional. Prefers this peer when possible</td>
</tr>
<tr>
<td>version <code>&lt;1-4&gt;</code> prefer</td>
<td>Optional. Configures a NTP version as preferred</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server <code>&lt;PEER-IP&gt;</code></td>
<td>Configures a NTP server association</td>
</tr>
<tr>
<td>prefer {version <code>&lt;1-4&gt;</code>}</td>
<td>Optional. Prefers this peer when possible</td>
</tr>
<tr>
<td>version <code>&lt;1-4&gt;</code> prefer</td>
<td>Optional. Configures a NTP version as preferred</td>
</tr>
<tr>
<td>version <code>&lt;1-4&gt;</code></td>
<td>Select the NTP version</td>
</tr>
</tbody>
</table>


Examples

rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.10
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
  ..............................................
ip dhcp trust
qos trust dscp
qos 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
  ntp server 172.16.10.10 prefer version 1
  misconfiguration-recovery-time 65
  noc update-interval 25
  ap300 00-15-70-63-4F-86 adopt
  ap300 00-15-70-63-4F-97 adopt
  ap300 00-A0-F8-CF-1E-DA adopt
  service pm sys-restart
  router ospf

Related Commands

no
- Disables or reverts settings to their default
### 7.1.55 offline-duration

**Profile Config Commands**

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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
offline-duration <5-43200>
```

**Parameters**

- `offline-duration <5-43200>`

<table>
<thead>
<tr>
<th>offline-duration &lt;5-43200&gt;</th>
<th>Specify a value from 5 - 43200 minutes. The default is 10 minutes.</th>
</tr>
</thead>
</table>

**Examples**

```bash
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)
### 7.1.56 power-config

**Profile Config Commands**

Configures the power option mode. Sets the amount of power that the access point draws.

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX

**Syntax**

- `power-config [af-option|at-option|mode]`
- `power-config [af-option|at-option] [range|throughput]`
- `power-config mode [auto|3af]`

**Parameters**

- **af-option**
  
  [range|throughput]

  Configures the 802.3.af power mode option. The options are:
  - range — Configures the af power range mode. This mode provides higher power but fewer transmission (tx) chains.
    
    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.
  
  - throughput — Configures the af power throughput mode. This mode provides lower power but has more tx chains. This is the default setting.
    
    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.

- **at-option**
  
  [range|throughput]

  Configures the 802.3 at power mode option. The options are:
  - range — Configures the at power range mode. This mode provides higher power but fewer tx chains.
    
    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.
  
  - throughput — Configures the at power throughput mode. This mode provides lower power but has more tx chains. This is the default setting.
    
    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.
power-config mode [auto|3af]

mode [auto|3af] Configures the AP power mode

- 3af – Forces an AP to power up in the 802.3af power mode
- auto – Sets the detection auto mode (default setting)

The automatic power-config mode enables an access point to automatically determine the best power configuration based on the available power budget.

Examples

rfs7000-37FABE(config-profile-defalut-rfs7000)#power-config af-option range
% Warning: AP must be restarted for power-management change to take effect.
rfs7000-37FABE(config-profile-defalut-rfs7000)#

rfs7000-37FABE(config-profile-defalut-rfs7000)#power-config at-option throughput
% Warning: AP must be restarted for power-management change to take effect.
rfs7000-37FABE(config-profile-defalut-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#power-config af-option range
% Error on default-rfs7000: AP power configuration not available for rfs7000 platform
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

no Reverts the power mode setting on this profile to default
7.1.57 preferred-controller-group

Profile Config Commands

Specifies the controller group preferred for adoption

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

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
ap300 00-15-70-63-4F-86 adopt
ap300 00-15-70-63-4F-97 adopt
ap300 00-A0-F8-CF-1E-DA adopt
service pm sys-restart
router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands
- no
  Removes the preferred controller group configuration
### 7.1.58 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
preferred-tunnel-controller <NAME>
```

**Parameters**

- `preferred-tunnel-controller <NAME>`

**Examples**

```
rfs7000-37FABE(config-profile-default-rfs7000)#preferred-tunnel-controller testtunnel
```

**Related Commands**

```
no
```

Removes the preferred tunnel configuration
7.1.59 radius

Profile Config Commands

Configures device level RADIUS authentication parameters

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
radius [nas-identifier|nas-port-id] <WORD>
```

Parameters

- `radius [nas-identifier|nas-port-id] <WORD>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas-identifier</td>
<td>Specifies the RADIUS Network Access Server (NAS) identifier attribute used by this device</td>
</tr>
<tr>
<td></td>
<td>&lt;WORD&gt; – Specifies the NAS identifier</td>
</tr>
<tr>
<td>nas-port-id</td>
<td>Specifies the RADIUS NAS port ID attribute used by this device</td>
</tr>
<tr>
<td></td>
<td>&lt;WORD&gt; – 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
7.1.60 remove-override

Profile Config Commands

Removes the offline-duration settings applied at the device level. When enabled, at the time of adoption, this feature removes offline-duration settings applied on the device, and profile-specific values are applied.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
remove-override offline-duration

Parameters
None

Examples
rfs4000-229D58 (config-profile-RFS4000test)#remove-override offline-duration
rfs4000-229D58 (config-profile-RFS4000test)#
7.1.61 rf-domain-manager

Profile Config Commands

Enables the RF Domain manager

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

rf-domain-manager [capable|priority <1-255>]

Parameters

- rf-domain-manager [capable|priority <1-255>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capable</td>
<td>Enables a device to become a site manager</td>
</tr>
<tr>
<td>priority &lt;1-255&gt;</td>
<td>Assigns a priority value for site manager selection</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
ap300 00-15-70-63-4F-86 adopt
ap300 00-15-70-63-4F-97 adopt
ap300 00-A0-F8-CF-1E-DA adopt
service pm sys-restart
preferred-tunnel-controller testtunnel
router ospf
rfs7000-37FABE(config-profile-default-rfs7000)#

Related Commands

- no Disables or reverts settings to their default
### 7.1.62 router

**Profile Config Commands**

Configures dynamic router protocol settings. For more details on router commands, see [ROUTER-MODE COMMANDS](#).

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
router ospf
```

**Parameters**

- router ospf

<table>
<thead>
<tr>
<th>ospf</th>
<th>Enables OSPF settings. Changes configuration mode to router mode</th>
</tr>
</thead>
</table>

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.

**Examples**

```plaintext
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
- `vrrp-state-check` Publish interface via OSPF only if the interface VRRP state is not BACKUP

```plaintext
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>no</th>
<th>Disables OSPF settings</th>
</tr>
</thead>
</table>

```plaintext
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```
7.1.63 **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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errdisable</td>
<td>Disables or shuts down 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</td>
</tr>
<tr>
<td>cause bpduguard</td>
<td>Specifies the reason for errdisable</td>
</tr>
<tr>
<td>interval &lt;10-1000000&gt;</td>
<td>specifies the interval after which a port is enabled</td>
</tr>
<tr>
<td>priority &lt;0-15&gt;</td>
<td>Specifies the number of instances required to configure MST. Select a value from 0-15.</td>
</tr>
<tr>
<td>priority &lt;0-61440&gt;</td>
<td>Sets the bridge priority to the specified value. Use the no parameter with this command to restore the default bridge priority value.</td>
</tr>
<tr>
<td>max-hops &lt;7-127&gt;</td>
<td>Sets the bridge priority in increments (Lower priority indicates greater likelihood of becoming root)</td>
</tr>
<tr>
<td>max-age &lt;6-40&gt;</td>
<td>Sets the bridge priority to the specified value. Use the no parameter with this command to restore the default bridge priority value.</td>
</tr>
<tr>
<td>max-hops &lt;7-127&gt;</td>
<td>Determines the maximum number of hops that are allowed in the spanning tree.</td>
</tr>
</tbody>
</table>

**spanning-tree mst</code>**

```
```

**errdisable recovery [cause bpduguard|interval <10-1000000>]**

- **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**

- **spanning-tree portfast [bpdufilter|bpduguard] default**

**Syntax**

```
spanning-tree portfast [bpdufilter|bpduguard] default
```

**Parameters**

- **spanning-tree portfast [bpdufilter|bpduguard] default**

  - **spanning-tree portfast [bpdufilter|bpduguard] default**

**Syntax**

```
```

**Parameters**

- **spanning-tree portfast [bpdufilter|bpduguard] default**

  - **spanning-tree portfast [bpdufilter|bpduguard] default**
### 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>
7.1.64 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 — AP300, 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, 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 a name.</td>
</tr>
</tbody>
</table>

Examples

rfs7000-37FABE(config-profile-default-rfs7000)#tunnel-controller testgroup

Related Commands

<table>
<thead>
<tr>
<th>no</th>
<th>Removes the configured the tunneled WLAN (extended VLAN) wireless controller or service platform’s name</th>
</tr>
</thead>
</table>
**7.1.65 use**

- **Profile Config Commands**

  Associates existing policies with this profile

  Supported in the following platforms:
  - Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
  - Wireless Controllers — RFS4000, RFS6000, RFS7000
  - Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax Profiles Mode**

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy|
captive-portal|client-identity-group|dhcp-server-policy|event-system-policy|
firewall-policy|global-assoc-list|management-policy|profile|radius-server-policy|
role-policy|routing-policy|wips-policy|critical-resource-policy]
```

**Syntax Device Mode**

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy|
captive-portal|client-identity-group|dhcp-server-policy|event-system-policy|
firewall-policy|global-assoc-list|management-policy|profile|radius-server-policy|
rf-domain|role-policy|routing-policy|wips-policy|critical-resource-policy|
smart-rf-policy|trustpoint]
```

---

**NOTE:** The following tables contain the `use` command parameters for the Profile and Device configuration modes.

### Parameters Profiles Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use auto-provisioning-policy</td>
<td>Associates an auto provisioning policy</td>
</tr>
<tr>
<td>&lt;POLICY-NAME&gt;</td>
<td>The specified policies should be existing and configured.</td>
</tr>
<tr>
<td>Use auto-provisioning-policy</td>
<td>Use auto-provisioning-policy &lt;POLICY-NAME&gt;</td>
</tr>
<tr>
<td>auto-provisioning-policy</td>
<td>&lt;POLICY-NAME&gt; – Specify the auto provisioning policy name.</td>
</tr>
<tr>
<td>bonjour-gw-forwarding-policy</td>
<td>Uses an existing Bonjour GW Forwarding policy with a profile or device</td>
</tr>
<tr>
<td>&lt;POLICY-NAME&gt;</td>
<td>&lt;POLICY-NAME&gt; – Specify the Bonjour GW Forwarding policy name (should be existing and configured).</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This feature is supported only on the RFS7000 and AP7131 devices.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>For more information on Bonjour GW Forwarding policy, see <code>bonjour-gw-forwarding-policy</code>.</td>
</tr>
<tr>
<td>captive-portal server</td>
<td>Configures access to a specified captive portal with this profile</td>
</tr>
<tr>
<td>&lt;CAPTIVE-PORTAL&gt;</td>
<td>&lt;CAPTIVE-PORTAL&gt; – Specify the captive portal name.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>For more information on Bonjour GW Forwarding policy, see <code>bonjour-gw-forwarding-policy</code>.</td>
</tr>
</tbody>
</table>
### Parameters Device Mode


#### use

Associates the following policies with this device:

- auto-provisioning-policy <POLICY-NAME>
  - Associates an auto provisioning policy
  - <POLICY-NAME> – Specify the auto provisioning policy name.

- captive-portal server <CAPTIVE-PORTAL>
  - Configures access to a specified captive portal
  - <CAPTIVE-PORTAL> – Specify the captive portal name.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identity</td>
<td>Associates an existing client identity group with this profile</td>
</tr>
<tr>
<td>&lt;CLIENT-IDENTITY-GROUP-NAME&gt;</td>
<td>• &lt;CLIENT-IDENTITY-GROUP-NAME&gt; – 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</td>
</tr>
<tr>
<td></td>
<td>client-identity and client-identity-group.</td>
</tr>
<tr>
<td>dhcp-server-policy</td>
<td>Associates a DHCP server policy</td>
</tr>
<tr>
<td>&lt;DHCP-POLICY&gt;</td>
<td>• &lt;DHCP-POLICY&gt; – Specify the DHCP server policy name.</td>
</tr>
<tr>
<td>event-system-policy</td>
<td>Associates an event system policy</td>
</tr>
<tr>
<td>&lt;EVENT-SYSTEM-POLICY&gt;</td>
<td>• &lt;EVENT-SYSTEM-POLICY&gt; – Specify the event system policy name.</td>
</tr>
<tr>
<td>firewall-policy</td>
<td>Associates a firewall policy</td>
</tr>
<tr>
<td>&lt;FW-POLICY&gt;</td>
<td>• &lt;FW-POLICY&gt; – Specify the firewall policy name.</td>
</tr>
<tr>
<td>global-assoc-list server</td>
<td>Associates the specified global association list with the controller profile</td>
</tr>
<tr>
<td>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</td>
<td>• &lt;GLOBAL-ASSOC-LIST-NAME&gt; – Specify the global association list name.</td>
</tr>
<tr>
<td></td>
<td>Once associated, the controller, using this profile, applies this association list to requests</td>
</tr>
<tr>
<td></td>
<td>received from all adopted APs. For more information on global association list, see</td>
</tr>
<tr>
<td></td>
<td>global-association-list.</td>
</tr>
<tr>
<td>management-policy</td>
<td>Associates a management policy</td>
</tr>
<tr>
<td>&lt;MNGT-POLICY&gt;</td>
<td>• &lt;MNGT-POLICY&gt; – Specify the management policy name.</td>
</tr>
<tr>
<td>radius-server-policy</td>
<td>Associates a device onboard RADIUS policy</td>
</tr>
<tr>
<td>&lt;RADIUS-POLICY&gt;</td>
<td>• &lt;RADIUS-POLICY&gt; – Specify the RADIUS policy name.</td>
</tr>
<tr>
<td>role-policy</td>
<td>Associates a role policy</td>
</tr>
<tr>
<td>&lt;ROLE-POLICY&gt;</td>
<td>• &lt;ROLE-POLICY&gt; – Specify the role policy name.</td>
</tr>
<tr>
<td>routing-policy</td>
<td>Associates a routing policy</td>
</tr>
<tr>
<td>&lt;ROUTING-POLICY&gt;</td>
<td>• &lt;ROUTING-POLICY&gt; – Specify the routing policy name.</td>
</tr>
<tr>
<td></td>
<td>This is not applicable to the NX45XX and NX65XX series profiles.</td>
</tr>
<tr>
<td>critical-resource-policy</td>
<td>Associates a critical resource monitoring policy</td>
</tr>
<tr>
<td>&lt;CRT-RESOURCE-POLICY&gt;</td>
<td>• &lt;CRT-RESOURCE-POLICY&gt; – Specify the critical resource policy name.</td>
</tr>
<tr>
<td></td>
<td>This is applicable only to the NX45XX and NX65XX series profiles.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>client-identity</td>
<td>Associates an existing client identity group with this device&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;CLIENT-IDENTITY-GROUP-NAME&gt;</code></td>
<td>- <code>&lt;CLIENT-IDENTITY-GROUP-NAME&gt;</code> – Specify the client identity group name.&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>For more information on the 'client-identity' and 'client-identity-group' commands, see &lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td><code>client-identity</code> and <code>client-identity-group</code>.</td>
</tr>
<tr>
<td>dhcp-server-policy</td>
<td>Associates a DHCP server policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;DHCP-POLICY&gt;</code></td>
<td>- <code>&lt;DHCP-POLICY&gt;</code> – Specify the DHCP server policy name.</td>
</tr>
<tr>
<td>event-system-policy</td>
<td>Associates an event system policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;EVENT-SYSTEM-POLICY&gt;</code></td>
<td>- <code>&lt;EVENT-SYSTEM-POLICY&gt;</code> – Specify the event system policy name.</td>
</tr>
<tr>
<td>firewall-policy</td>
<td>Associates a firewall policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;FW-POLICY&gt;</code></td>
<td>- <code>&lt;FW-POLICY&gt;</code> – Specify the firewall policy name.</td>
</tr>
<tr>
<td>global-assoc-list server</td>
<td>Associates the specified global association list with the device (controller)&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</code></td>
<td>- <code>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</code> – Specify the global association list name.&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>Once associated, the controller applies this association list to requests received from all&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>adopted APs. For more information on global assoc it ion list, see <code>global-association-list</code>.</td>
</tr>
<tr>
<td>igmp-snoop-policy</td>
<td>Associates an IGMP snoop policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;IGMP-POLICY&gt;</code></td>
<td>- <code>&lt;IGMP-POLICY&gt;</code> – Specify the IGMP snoop policy name.</td>
</tr>
<tr>
<td>management-policy</td>
<td>Associates a management policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;MNGT-POLICY&gt;</code></td>
<td>- <code>&lt;MNGT-POLICY&gt;</code> – Specify the management policy name.</td>
</tr>
<tr>
<td>profile</td>
<td>Associates a profile with this device&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;PROFILE-NAME&gt;</code></td>
<td>- <code>&lt;PROFILE-NAME&gt;</code> – Specify the profile name.</td>
</tr>
<tr>
<td>radius-server-policy</td>
<td>Associates a device onboard RADIUS policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;RADIUS-POLICY&gt;</code></td>
<td>- <code>&lt;RADIUS-POLICY&gt;</code> – Specify the RADIUS policy name.</td>
</tr>
<tr>
<td>rf-domain</td>
<td>Associates an RF Domain&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;RF-DOMAIN-NAME&gt;</code></td>
<td>- <code>&lt;RF-DOMAIN-NAME&gt;</code> – Specify the RF Domain name.</td>
</tr>
<tr>
<td>role-policy</td>
<td>Associates a role policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;ROLE-POLICY&gt;</code></td>
<td>- <code>&lt;ROLE-POLICY&gt;</code> – Specify the role policy name.</td>
</tr>
<tr>
<td>routing-policy</td>
<td>Associates a routing policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;ROUTING-POLICY&gt;</code></td>
<td>- <code>&lt;ROUTING-POLICY&gt;</code> – Specify the routing policy name.</td>
</tr>
<tr>
<td></td>
<td>This is not applicable to the NX45XX and NX65XX series devices.</td>
</tr>
<tr>
<td>wips-policy</td>
<td>Associates a WIPS policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;WIPS-POLICY&gt;</code></td>
<td>- <code>&lt;WIPS-POLICY&gt;</code> – Specify the WIPS policy name.</td>
</tr>
<tr>
<td>critical-resource-policy</td>
<td>Associates a critical resource monitoring policy&lt;br&gt;&lt;br&gt;</td>
</tr>
<tr>
<td><code>&lt;CRT-RESOURCE-POLICY&gt;</code></td>
<td>- <code>&lt;CRT-RESOURCE-POLICY&gt;</code> – Specify the critical resource policy name.</td>
</tr>
<tr>
<td></td>
<td>This is applicable only to the NX45XX and NX65XX series service platforms.</td>
</tr>
</tbody>
</table>
### smart-rf-policy

| `<SMART-RF-POLICY>` | Associates a Smart RF policy  
|---------------------|-------------------------------|
|                     | • `<SMART-RF-POLICY>` – Specify the Smart RF policy name.  
|                     | This is applicable only to the NX45XX and NX65XX series devices. |

### trustpoint

| `<TRUSTPOINT-NAME>` | Associates a trustpoint  
|---------------------|--------------------------|
|                     | • `<TRUSTPOINT-NAME>` – Specify the trustpoint name.  
|                     | This is applicable only to the NX45XX and NX65XX series devices. |

### Examples

```bash
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

| `no` | Disassociates a specified policy from this profile |
7.1.66 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 — AP300, 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, 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 [<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|pppoe1|vlan <1-4094>|wwan1]

vrrp <1-255> monitor [<IP-NAME>|critical-resource|pppoe1|vlan|wwan1]

vrrp <1-255> monitor [<IP-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>vrrp &lt;1-255&gt;</th>
<th>Configures the virtual router ID from 1-255. Identifies the virtual router the packet is reporting status for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>delta-priority &lt;1-253&gt;</td>
<td>Configures the priority to decrement (local link monitoring and critical resource monitoring) or increment (critical resource monitoring)</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-253&gt; – Specify the delta priority level from 1-253.</td>
</tr>
<tr>
<td>description &lt;LINE&gt;</td>
<td>Configures a text description for the virtual router to further distinguish it from other routers with similar configuration</td>
</tr>
<tr>
<td></td>
<td>• &lt;LINE&gt; – Provide a description (a string from 1-64 characters in length)</td>
</tr>
<tr>
<td>ip &lt;IP-ADDRESSES&gt;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP-ADDRESSES&gt; – Specify the IP address(es) in the A.B.C.D format.</td>
</tr>
<tr>
<td></td>
<td>This configuration triggers VRRP operation.</td>
</tr>
<tr>
<td>preempt {delay &lt;1-65535&gt;}</td>
<td>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 enabled by default.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>priority &lt;1-254&gt;</td>
<td>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).</td>
</tr>
<tr>
<td>sync-group</td>
<td>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.</td>
</tr>
<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>interface &lt;INTERFACE-NAME&gt;</td>
<td>Enables VRRP on the selected SVI interface</td>
</tr>
<tr>
<td></td>
<td>• &lt;INTERFACE-NAME&gt; – Enables VRRP on the VLAN interface specified by the &lt;INTERFACE-NAME&gt; parameter</td>
</tr>
<tr>
<td></td>
<td>• ge &lt;1-4&gt; – Enables VRRP on the specified GigabitEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• me1 – Enables VRRP on the FastEthernet interface</td>
</tr>
<tr>
<td></td>
<td>• pppoe1 – Enables VRRP on the PPP over Ethernet interface</td>
</tr>
<tr>
<td></td>
<td>• port-channel &lt;1-2&gt; – Enables VRRP on the port channel interface</td>
</tr>
<tr>
<td></td>
<td>• vlan &lt;1-4094&gt; – Enables VRRP on the specified VLAN interface</td>
</tr>
<tr>
<td></td>
<td>• wwan1 – Enables VRRP on the Wireless WAN interface</td>
</tr>
<tr>
<td>vrrp &lt;1-255&gt; monitor critical-resource &lt;CRM-NAME1&gt; &lt;CRM-NAME2&gt; &lt;CRM-NAME3&gt; &lt;CRM-NAME4&gt; {action [decrement-priority</td>
<td>increment-priority] {&lt;IF-NAME&gt;</td>
</tr>
<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 Critical Resource Monitoring (CRM)</td>
</tr>
</tbody>
</table>
### 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. |

### action

<table>
<thead>
<tr>
<th><code>[decrement-priority]</code></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[increment-priority]</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;decrement-priority&gt;</code></td>
<td>decrements the priority of virtual router on critical resource down event</td>
</tr>
<tr>
<td><code>&lt;increment-priority&gt;</code></td>
<td>increments the priority of virtual router on critical resource down event</td>
</tr>
</tbody>
</table>

### `<IF-NAME>`

<table>
<thead>
<tr>
<th>Optional. Enables interface monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IF-NAME&gt;</code></td>
</tr>
</tbody>
</table>

### pppoe1

| Optional. Enables Point-to-Point Protocol (PPP) over Ethernet interface monitoring  |

### vlan <1-4094>

<table>
<thead>
<tr>
<th>Optional. Enables VLAN (switched virtual interface) interface monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-4094&gt;</code></td>
</tr>
</tbody>
</table>

### wwan1

| Optional. Enables Wireless WAN interface monitoring  |

### vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]

<table>
<thead>
<tr>
<th>Configures the VRRP advertisements time interval. This is the interval a master sends out advertisements on each of its configured VLANs.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-255&gt;</code></td>
</tr>
<tr>
<td><code>&lt;centiseconds &lt;25-4095&gt;</code></td>
</tr>
<tr>
<td><code>&lt;msec &lt;250-999&gt;</code></td>
</tr>
</tbody>
</table>

### vrrp version [2|3]

<table>
<thead>
<tr>
<th>Configures one of the following VRRP versions:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>2</code></td>
</tr>
<tr>
<td><code>3</code></td>
</tr>
<tr>
<td>The VRRP version determines the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.</td>
</tr>
</tbody>
</table>
**Examples**

```plaintext
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
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><strong>no</strong></td>
<td>Reverts VRRP settings</td>
</tr>
</tbody>
</table>
7.1.67 **wep-shared-key-auth**

- **Profile Config Commands**

Enables support for 802.11 WEP shared key authentication

Supported in the following platforms:
- Access Points — AP300, 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, NX81XX, NX9000, NX9500, NX9510, NX9600

**Syntax**
wep-shared-key-auth

**Parameters**
None

**Examples**
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 me1
  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 | Disable support for 802.11 WEP shared key authentication |
7.1.68 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

service [critical-resource|fast-switching|enable|global-association-list|meshpoint|pm|power-config|radius|rss-timeout|watchdog|wireless|show]

service critical-resource port-mode-source-ip <IP>

service cluster master selection immediate

service enable [l2tpv3|pppoe|radius]

service global-association-list blacklist-interval <1-65535>

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 rss-timeout <0-86400>

service watchdog

service wireless [ap300|ap650|client|cred-cache-sync|test|wispe-controller-port]

service wireless ap300 [image <FILE>|version]

service wireless ap650 legacy-auto-update-image <FILE>

service wireless client tx-deauth on-radar-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 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:

service fast-switching

Parameters
- service cluster master-election immediate

<table>
<thead>
<tr>
<th>service cluster master-election immediate</th>
<th>Allows the master-election to complete more quickly.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• master-election — Configures master-election</td>
</tr>
<tr>
<td></td>
<td>• immediate — Cluster master election completes immediately when only one active cluster member is available</td>
</tr>
</tbody>
</table>
- `service critical-resource port-mode-source-ip <IP>`
  
  **critical-resource port-mode-source-ip <IP>**  Hard codes a source IP for critical resource management

- `service enable [l2tpv3|pppoe|radiusd]`
  
  **service enable l2tpv3**  Enables/disables L2TPv3 on this profile  
  This feature is not supported on AP622, AP650, AP6522, AP6562, AP71XX, AP81XX, AP82XX, RFS4000, RFS6000, and RFS7000.  
  It is supported only on AP621, AP6511, and AP6521.

  **service enable pppoe**  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.

  **service enable radiustr**  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.

- `service global-association-list blacklist-interval <1-65535>`
  
  **service global-association-list blacklist-interval <1-65535>**  Configures global association list related parameters  
  **blacklist-interval <1-65535>**  Configures the period for which a client is blacklisted. A client is considered blacklisted after being denied access by the server.  
  • `<1-65535>` – Specify a value from 1 - 65535 seconds.

- `service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-4>|port-channel <1-2>]

  **meshpoint loop-prevention-port**  Limits meshpoint loop prevention to a single port  
  **<L2-INTERFACE-NAME>**  Limits meshpoint loop prevention on a specified Ethernet interface  
  • `<L2-INTERFACE-NAME>` – Specify the layer 2 Ethernet interface name.

  **ge <1-4>**  Limits meshpoint loop prevention on a specified GigabitEthernet interface  
  • `ge <1-4>` – Specify the GigabitEthernet interface index from 1 - 4.

  **port-channel <1-2>**  Limits meshpoint loop prevention on a specified port-channel interface  
  • `port-channel <1-2>` – Specify the port-channel interface index from 1 - 2.

- `service pm sys-restart

  pm sys-restart  Enables the process monitor (PM) to restart the system when a process fails

- `service power-config [3af-out|force-3at]

  **power-config 3af-out**  Enables LLDP power negotiation, but uses 3af power

  **power-config force-3at**  Disables LLDP negotiation and force 802.3at power configuration
- `service radius dynamic-authorization additional-port <1-65535>`

  Configures an additional UDP port used by the device to listen for dynamic authorization messages.
  - `<1-65535>` – Specify a value from 1 - 65535.
  The Cisco Identity Services Engine (ISE) server uses port 1700.

- `service rss-timeout <0-86400>`

  Configures the duration, in seconds, for which an adopted access point will continue to provide wireless functions even after losing controller adoption.
  - `<0-86400>` – Specify a value from 0 - 86400 seconds.

- `service watchdog`

  Enables/disables 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.

- `service wireless ap300 [image <FILE>|version]`

  Invokes AP300 related service commands.
  - `<FILE>` – Provides the path and name of the AP300 image file (for example, flash:/ap.img)

- `service wireless ap650 legacy-auto-update-image <FILE>`

  Invokes AP650 related service commands.
  - `<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.
  Enables/disables access points to transmit deauth to clients when changing channels on radar detection.

- `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.
  - `<never>` – Specify a value from 30 - 864000 seconds.
  - `<partial>` – Enables partial synchronization of parameters for associated clients, with credential cache close to aging out.
- service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24,36,48,54,mcs0,mcs1,............mcs23]
  wireless test Configures the serviceability parameters used for testing
  [max-rate|min-rate] Configures the maximum and minimum data rates for clients using rate-scaling
  [1,2,5.5,.,mcs23] Select the maximum and minimum data rates applicable.

- service wireless test max-retries <0-15>
  wireless test Configures the serviceability parameters used for testing
  max-retries <0-15> Configures the maximum number of retries per packet

- service wireless wispe-controller-port <1-65535>
  wispe-controller-port <1-65535> Resets the Wireless Switch Protocol Enhanced (WISPe) controller port. This is the UDP port used to listen for WISPe.
  • <1-65535> – Specify a value from 1-65535.

- service show cli
  show cli Displays running system configuration details
  • cli – Displays the CLI tree of the current mode

- service fast-switching
  fast-switching Enables fast switching of packets in the hardware
  Use the no > service > fast-switching to disable this feature.
  Fast switching can be enabled and disabled on the NX45XX and NX65XX series service platform.

Examples
rfs7000-37FABE(config-profile-testrfs71xx)#service radius dynamic-authorization additional-port 1700
rfs7000-37FABE(config-profile-testrfs71xx)#
rfs7000-37FABE(config-profile-testrfs71xx)#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
  --More--
rfs7000-37FABE(config-profile-testrfs71xx)#

Related Commands
  no Removes or resets service command parameters
### 7.1.69 slot

**Profile Config Commands**

Assigns a Peripheral Component Interconnect (PCI) expansion slot for Team-URC VM or WiNG support.

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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4&gt;</td>
<td>Select the slot from 1 - 4. The command selects the slot and enters its configuration mode.</td>
</tr>
</tbody>
</table>

In the slot configuration mode, do the following:
- **assign** — Assigns the selected slot to either TEAM-URC VM or WiNG support
- **team-centro** — Assigns the selected slot to TEAM-URC VM (IP PBX)
- **wing** — Assigns the selected slot to WiNG

**Note:** The `show > slot` command displays slots and their assignment details (type and status).

**Examples**

```bash	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

```bash	nx4500-5CFA2B(config-profile testNX45XX-slot-1)#
```

```bash	nx4500-5CFA2B(config-profile testNX45XX-slot-1)#assign team-centro
```

```bash	nx4500-5CFA2B(config-profile testNX45XX-slot-1)#show context
```

```bash	nx4500-5CFA2B(config-profile testNX45XX-slot-1)#assign team-centro
```

```bash	nx4500-5CFA2B(config-device B4-C7-99-5C-FA-2B-slot-1)#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>team-centro</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(config-device B4-C7-99-5C-FA-2B-slot-1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the PCI expansion slot assignment for Team-URC VM or WiNG support</td>
</tr>
</tbody>
</table>
7.2 Device Config Commands

Use the (config) instance to configure device specific parameters.

To navigate to this instance, use the following commands:

```conf
<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-site**: Set system's adoption site.
- **alias**: Alias.
- **ap300**: Adopt/unadopt AP300 device to this profile/device.
- **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.
- **autostartup**: Autoinstall settings.
- **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.
- **device-upgrade**: Device firmware upgrade.
- **dot1x**: 802.1X.
- **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.
- **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).
- **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

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

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

Set the flag to reevaluate autoprovisioning policy everytime

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 the stats related setting

Configure the timezone

Assign a trustpoint to a service

Tunnel Controller group this controller belongs to

Set setting to use

VRRP configuration

Enable support for 802.11 WEP shared key authentication

Clears the display screen

Commit all changes made in this
**Table 7.24 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 7-10</td>
</tr>
<tr>
<td>adoption-site</td>
<td>Sets the device's adoption site name</td>
<td>page 7-384</td>
</tr>
<tr>
<td>alias</td>
<td>Configures network, VLAN, and service aliases on a device</td>
<td>page 7-12</td>
</tr>
<tr>
<td>ap300</td>
<td>Enables adoption of AP300s by a wireless controller or service platform</td>
<td>page 7-18</td>
</tr>
<tr>
<td>area</td>
<td>Sets the name of area where the system is deployed</td>
<td>page 7-385</td>
</tr>
<tr>
<td>arp</td>
<td>Configures ARP parameters</td>
<td>page 7-20</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enables the automatic recognition of devices pending adoption</td>
<td>page 7-22</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 7-23</td>
</tr>
<tr>
<td>autoinstall</td>
<td>Aut Installs firmware image and configuration setup parameters</td>
<td>page 7-25</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures Ethernet Bridging parameters</td>
<td>page 7-27</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures captive portal advanced Web page upload on this profile</td>
<td>page 7-47</td>
</tr>
<tr>
<td>cdp</td>
<td>Operates CDP on the device</td>
<td>page 7-48</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures channel list advertised to wireless clients</td>
<td>page 7-386</td>
</tr>
<tr>
<td>cluster</td>
<td>Sets cluster configuration</td>
<td>page 7-49</td>
</tr>
<tr>
<td>configuration-persistence</td>
<td>Enables configuration persistence across reloads</td>
<td>page 7-51</td>
</tr>
<tr>
<td>contact</td>
<td>Sets contact information</td>
<td>page 7-387</td>
</tr>
<tr>
<td>controller</td>
<td>Configures a WLAN’s wireless controller or service platform</td>
<td>page 7-52</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures wireless controller or service platform’s country code</td>
<td>page 7-388</td>
</tr>
<tr>
<td>critical-resource</td>
<td>Monitors user configured IP addresses and logs their status</td>
<td>page 7-55</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>crypto</td>
<td>Configures data encryption protocols and settings</td>
<td>page 7-59</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings on this device</td>
<td>page 7-119</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures 802.1x standard authentication controls</td>
<td>page 7-122</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 7-124</td>
</tr>
<tr>
<td>email-notification</td>
<td>Configures e-mail notification</td>
<td>page 7-125</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Checks the device firmware version before attempting connection</td>
<td>page 7-127</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 configures its settings,</td>
<td>page 7-128</td>
</tr>
<tr>
<td>events</td>
<td>Displays system event messages</td>
<td>page 7-130</td>
</tr>
<tr>
<td>export</td>
<td>Enables export of startup.log file after every boot</td>
<td>page 7-131</td>
</tr>
<tr>
<td>floor</td>
<td>Sets the building floor where the system is deployed</td>
<td>page 7-389</td>
</tr>
<tr>
<td>geo-coordinates</td>
<td>Configures the geographic coordinates for this device</td>
<td>page 7-390</td>
</tr>
<tr>
<td>gre</td>
<td>Enables GRE tunneling on this device</td>
<td>page 7-134</td>
</tr>
<tr>
<td>hostname</td>
<td>Sets a system’s network name</td>
<td>page 7-391</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enables HTTP analysis on this device</td>
<td>page 7-144</td>
</tr>
<tr>
<td>interface</td>
<td>Selects an interface to configure</td>
<td>page 7-149</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP components</td>
<td>page 7-302</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 7-311</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>Configures L3e Lite Table with this profile</td>
<td>page 7-313</td>
</tr>
<tr>
<td>layout-coordinates</td>
<td>Configures layout coordinates</td>
<td>page 7-392</td>
</tr>
<tr>
<td>led</td>
<td>Turns LEDs on or off</td>
<td>page 7-314</td>
</tr>
<tr>
<td>led-timeout</td>
<td>Configures the LED-timeout timer in the device or profile configuration mode</td>
<td>page 7-315</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Enables legacy device firmware to auto downgrade</td>
<td>page 7-316</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto updates AP650 and AP71XX legacy device firmware</td>
<td>page 7-317</td>
</tr>
<tr>
<td>license</td>
<td>Adds a license for a device’s features</td>
<td>page 7-393</td>
</tr>
<tr>
<td>lldp</td>
<td>Configures Link Layer Discovery Protocol (LLDP) settings for this profile</td>
<td>page 7-318</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configures load balancing parameters.</td>
<td>page 7-319</td>
</tr>
<tr>
<td>location</td>
<td>Configures the location the system is deployed</td>
<td>page 7-395</td>
</tr>
</tbody>
</table>
### Table 7.24 Device-Configuration-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging</td>
<td>Enables message logging</td>
<td>page 7-324</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Configures the MAC address table</td>
<td>page 7-326</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables 802.1x authentication of hosts on this device</td>
<td>page 7-328</td>
</tr>
<tr>
<td>mac-name</td>
<td>Configures MAC name to name mappings</td>
<td>page 7-396</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Configures memory profile used on the device</td>
<td>page 7-331</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configures meshpoint device parameters</td>
<td>page 7-332</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configures meshpoint monitoring interval</td>
<td>page 7-333</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Configures the minimum device connectivity verification time</td>
<td>page 7-334</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol commands</td>
<td>page 7-335</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Verifies device connectivity after a configuration is received</td>
<td>page 7-341</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configures a neighbor inactivity timeout</td>
<td>page 7-342</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configures the neighbor information exchange interval</td>
<td>page 7-397</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or resets values to their default settings</td>
<td>page 7-398</td>
</tr>
<tr>
<td>noc</td>
<td>Configures NOC settings</td>
<td>page 7-347</td>
</tr>
<tr>
<td>ntp</td>
<td>Configure the NTP server settings</td>
<td>page 7-348</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 7-350</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configures WLAN RF Domain level overrides</td>
<td>page 7-402</td>
</tr>
<tr>
<td>power-config</td>
<td>Configures power mode features</td>
<td>page 7-351</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 7-353</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 7-354</td>
</tr>
<tr>
<td>radius</td>
<td>Configures device-level RADIUS authentication parameters</td>
<td>page 7-355</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides</td>
<td>page 7-403</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Enables the RF Domain manager</td>
<td>page 7-357</td>
</tr>
<tr>
<td>router</td>
<td>Configures dynamic router protocol settings</td>
<td>page 7-358</td>
</tr>
</tbody>
</table>
### Table 7.24 Device-Configuration-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsa-key</td>
<td>Assigns a RSA key to SSH</td>
<td>page 7-405</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server</td>
<td>page 7-406</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Enables spanning tree commands</td>
<td>page 7-359</td>
</tr>
<tr>
<td>timezone</td>
<td>Configures wireless controller or service platform’s time zone settings</td>
<td>page 7-407</td>
</tr>
<tr>
<td>trustpoint</td>
<td>Assigns a trustpoint to a service</td>
<td>page 7-408</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Configures the tunneled WLAN (extended VLAN) wireless controller or service</td>
<td>page 7-362</td>
</tr>
<tr>
<td>use</td>
<td>Defines the settings used with this command</td>
<td>page 7-363</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configures VRRP group settings</td>
<td>page 7-367</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enables support for 802.11 WEP shared key authentication</td>
<td>page 7-371</td>
</tr>
<tr>
<td>mirror</td>
<td>Enables port mirroring on GE ports. This command is supported only on the</td>
<td>page 7-409</td>
</tr>
<tr>
<td></td>
<td>NX4524 and NX6524 series service platforms.</td>
<td></td>
</tr>
<tr>
<td>raid</td>
<td>Enables alarm on the array. This command is supported only on the NX9500</td>
<td>page 7-411</td>
</tr>
<tr>
<td></td>
<td>series service platform.</td>
<td></td>
</tr>
<tr>
<td>slot</td>
<td>Assigns a physical slot for running Team-URC VM on this profile/device.</td>
<td>page 7-376</td>
</tr>
<tr>
<td></td>
<td>This feature is support only on the NX45XX and NX65XX series service platforms.</td>
<td></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 — AP300, 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, 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 TestEcoSpace3B
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

**Related Commands**

- no | Disables or reverts settings to their default
7.2.2 area

- **Device Config Commands**

  Sets the area where the system is deployed

  Supported in the following platforms:
  - Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`area <AREA-NAME>`

**Parameters**

- `area <AREA-NAME>`

**Examples**

```plaintext
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**

- `no` Disables or reverts settings to their default
7.2.3 channel-list

- **Device Config Commands**

Configures the channel list advertised to wireless clients

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
channel-list [2.4GHz|5GHz|dynamic]
cchannel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]
```

**Parameters**

- **channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz &lt;CHANNEL-LIST&gt;</td>
<td>Configures the channel list advertised by radios operating in 2.4 GHz</td>
</tr>
<tr>
<td>5GHz &lt;CHANNEL-LIST&gt;</td>
<td>Configures the channel list advertised by radios operating in 5.0 GHz</td>
</tr>
<tr>
<td>dynamic</td>
<td>Enables dynamic (neighboring access point based) update of configured channel list</td>
</tr>
</tbody>
</table>

**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-ap71xx
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

Defines an administrative contact for a deployed device

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
contact <WORD>

Parameters
- contact <WORD>

Examples
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#contact company

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 company
  channel-list 2.4GHz 1,2

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.

Supported in the following platforms:

- **Access Points** — AP300, 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, 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 company
    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>no</td>
<td>Removes the configured country code</td>
</tr>
</tbody>
</table>
7.2.6 floor

*Device Config Commands*

Sets the building floor where the device is deployed

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
floor <FLOOR-NAME>
```

**Parameters**

- `floor <FLOOR-NAME>`

**Examples**

```
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 RMZEcospace
floor 5thfloor
contact company
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>

Parameters
- geographic 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
rfs4000-229D58(config-device-00-23-68-22-9D-58)#

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
geo-coordinates -90.0000 166.0000
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
- no | Removes device's geographic coordinates
7.2.8 hostname

Device Config Commands

Sets the system's network name

Supported in the following platforms:

- Access Points — AP300, 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, 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 company
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 — AP300, 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, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;-4096.0-4096.0&gt;</code></td>
<td>Specify the X coordinate from -4096 - 4096.0</td>
</tr>
<tr>
<td><code>&lt;-4096.0-4096.0&gt;</code></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 2
```

```
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
contact company
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 device’s layout co-ordinates</td>
</tr>
</tbody>
</table>
7.2.10 license

Device Config Commands

Adds a license pack on the device for the specified feature (AP/AAP/ADSEC/ADVANCED-WIPS/HTANLT/SMART-CACHE).

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

license <WORD> <LICENSE-KEY>

Parameters

- license <WORD> <LICENSE-KEY>

<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Specify the feature name (AP/AAP/ADSEC/ADVANCED-WIPS/HTANLT/SMART-CACHE) for which license is added</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;LICENSE-KEY&gt;</td>
<td>Specify the license key</td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#license ap aplicensekey@123 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 Block3B
  no contact
  country-code us
  channel-list 2.4GHz 1,2
  mac-name 00-04-96-4A-A7-08 5.4TestAP
  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/ADVANCED-WIPS/HTANLT/SMART-CACHE) for which license is to be added

nx6524-858126(config-device-5C-0E-8B-85-81-26)#license SMART-CACHE
29bedfa30cf4a5bcd20cd8815e00c948ddf26814e8346ef6f9e884832a7a49b349e6938f63ecf653

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 : 11185520500065
Device Licenses:
  AP-LICENSE
    String : 29bedfa30cf4a5bce0c732a20e39f728ddf26814e8346ef6739f3ee2b1691d10246de8a11e439131
    ... HOTSPOT-ANALYTICS
    String : 29bedfa30cf4a5bcdf83ad26e814f39dddf26814e8346ef6f429383a6d51ac549e6938f63ecf653
  SMART-CACHE
    String : 29bedfa30cf4a5bcdc20cd8815e00c948ddf26814e8346ef6f9e884832a7a49b349e6938f63ecf653
--More--
nx6524-858126(config-device-SC-0E-8B-85-81-26)#
7.2.11 location

Device Config Commands

Sets the location where a managed device is deployed

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

location <WORD>

Parameters

- location <WORD>

Examples

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#location Block3B

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 Block3B
  contact company country-code us
  channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

Related Commands

no

Removes a managed device's location
7.2.12 **mac-name**

*Device Config Commands*

Configures a MAC name for mappings

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mac-name <MAC> <NAME>
```

**Parameters**

- `mac-name <MAC> <NAME>`

  - `<MAC>` — Configures a MAC address for the device
  - `<NAME>` — Set the 'friendly' name used for this MAC address

**Examples**

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#mac-name 00-04-96-4A-A7-08 5.4TestAP
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 RMZEcospae
  floor 5thfloor
  layout-coordinates 1.0 2.0
  location Block3B
  contact company country-code us
  channel-list 2.4GHz 1,2
  mac-name 00-04-96-4A-A7-08 5.4TestAP
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

| `no` | Removes the device’s friendly name to MAC address mapping |
7.2.13 **neighbor-info-interval**

*Device Config Commands*

Configures neighbor information exchange interval.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
neighbor-info-interval <1-100>
```

**Parameters**

- `neighbor-info-interval <1-100>`

<table>
<thead>
<tr>
<th>neighbor-info-interval &lt;1-100&gt;</th>
<th>Sets neighbor information exchange interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;1-100&gt;</code> – Specify a value from 1 - 100 seconds.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#neighbor-info-interval 50
```

```
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 RMZEcospase
  floor 5thfloor
  layout-coordinates 1.0 2.0
  location Block3B
  contact company
country-code us
channel-list 2.4GHz 1,2
mac-name 00-04-96-4A-A7-08 5.4TestAP
neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

| `no` | Removes or reverts the device's settings |
7.2.14 **no**

*Device Config Commands*

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [adopter-auto-provisioning-policy-lookup|adoption-site|ap300|area|arp|
    auto-learn-staging-config|autoinstall|bridge|cdp|channel-list|cluster|
    configuration-persistence|contact|controller|country-code|critical-resource|
    crypto|device-upgrade|dot1x|dscp-mapping|email-notification|environmental-sensor|
    events|export|floor|geo-coordinates|gre|hostname|http-analyze|interface|
    ip|l2tpv3|13-lite-table|layout-coordinates|led|legacy-auto-downgrade|
    legacy-auto-update|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|
    network-alias|noc|ntp|override-wlan|power-config|preferred-controller-group|
    preferred-tunnel-controller|radius|rf-domain-manager|router|rsa-key|sensor-server|
    slot|spanning-tree|timezone|trustpoint|tunnel-controller|use|vrrp|
    wep-shared-key-auth|service]
```

**Parameters**

None

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</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 or device</td>
</tr>
<tr>
<td>adoption-site</td>
<td>Sets the device’s adoption site name</td>
</tr>
<tr>
<td>alias</td>
<td>Creates a network, VLAN, and service alias and enters its configuration mode</td>
</tr>
<tr>
<td>ap300</td>
<td>Enables adoption of AP300s by a profile</td>
</tr>
<tr>
<td>area</td>
<td>Sets the name of area where the system is deployed</td>
</tr>
<tr>
<td>arp</td>
<td>Configures ARP parameters</td>
</tr>
<tr>
<td>auto-learn-staging-config</td>
<td>Enables the automatic recognition of devices pending adoption</td>
</tr>
<tr>
<td>autoinstall</td>
<td>Autoinstalls firmware image and configuration setup parameters</td>
</tr>
<tr>
<td>bridge</td>
<td>Configures Ethernet Bridging parameters</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cdp</td>
<td>Operates CDP on the device</td>
</tr>
<tr>
<td>channel-list</td>
<td>Configures channel list advertised to wireless clients</td>
</tr>
<tr>
<td>cluster</td>
<td>Sets cluster configuration</td>
</tr>
<tr>
<td>configuration-</td>
<td>Enables configuration persistence across reloads</td>
</tr>
<tr>
<td>persistence</td>
<td></td>
</tr>
<tr>
<td>contact</td>
<td>Sets contact information</td>
</tr>
<tr>
<td>controller</td>
<td>Configures controller WLAN settings</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures the two digit country code for legal operation</td>
</tr>
<tr>
<td>crypto</td>
<td>Configures crypto settings</td>
</tr>
<tr>
<td>device-upgrade</td>
<td>Configures device firmware upgrade settings on this device</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures 802.1x standard authentication controls</td>
</tr>
<tr>
<td>dscp-mapping</td>
<td>Configures IP Differentiated Services Code Point (DSCP) to 802.1p priority mapping for untagged frames</td>
</tr>
<tr>
<td>email-notification</td>
<td>Configures e-mail notification</td>
</tr>
<tr>
<td>enforce-version</td>
<td>Checks the device firmware version before attempting connection</td>
</tr>
<tr>
<td>environmental-</td>
<td>Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configures its settings,</td>
</tr>
<tr>
<td>sensor</td>
<td></td>
</tr>
<tr>
<td>events</td>
<td>Displays system event messages</td>
</tr>
<tr>
<td>export</td>
<td>Enables export of startup.log file after every boot</td>
</tr>
<tr>
<td>floor</td>
<td>Sets the building floor where the system is deployed</td>
</tr>
<tr>
<td>geo-coordinates</td>
<td>Configures the geographic coordinates for this device</td>
</tr>
<tr>
<td>gre</td>
<td>Enables GRE tunneling on this profile</td>
</tr>
<tr>
<td>hostname</td>
<td>Sets a system’s network name</td>
</tr>
<tr>
<td>http-analyze</td>
<td>Enables HTTP analysis on this device</td>
</tr>
<tr>
<td>interface</td>
<td>Selects an interface to configure</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP components</td>
</tr>
<tr>
<td>l2tpv3</td>
<td>Defines the L2TP protocol for tunneling layer 2 payloads using VPNs</td>
</tr>
<tr>
<td>l3e-lite-table</td>
<td>Configures L3e lite table aging time</td>
</tr>
<tr>
<td>layout-coordinates</td>
<td>Configures layout coordinates</td>
</tr>
<tr>
<td>led</td>
<td>Turns LEDs on or off</td>
</tr>
<tr>
<td>legacy-auto-downgrade</td>
<td>Enables legacy device firmware to auto downgrade</td>
</tr>
<tr>
<td>legacy-auto-update</td>
<td>Auto updates AP650 and AP71XX legacy device firmware</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lldp</td>
<td>Configures LLDP settings for this profile</td>
</tr>
<tr>
<td>load-balancing</td>
<td>Configures load balancing parameters</td>
</tr>
<tr>
<td>location</td>
<td>Configures the location the system is deployed</td>
</tr>
<tr>
<td>logging</td>
<td>Enables message logging</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>Configures the MAC address table</td>
</tr>
<tr>
<td>mac-auth</td>
<td>Enables 802.1x authentication of hosts on this device</td>
</tr>
<tr>
<td>mac-name</td>
<td>Configures MAC name to name mappings</td>
</tr>
<tr>
<td>memory-profile</td>
<td>Configures device’s memory profile</td>
</tr>
<tr>
<td>meshpoint-device</td>
<td>Configures device’s meshpoint parameters</td>
</tr>
<tr>
<td>meshpoint-monitor-interval</td>
<td>Configures meshpoint monitoring interval on the device</td>
</tr>
<tr>
<td>min-misconfiguration-recovery-time</td>
<td>Configures the minimum connectivity verification time</td>
</tr>
<tr>
<td>mint</td>
<td>Configures MiNT protocol commands</td>
</tr>
<tr>
<td>mirror</td>
<td>Enables port mirroring on a device</td>
</tr>
<tr>
<td>misconfiguration-recovery-time</td>
<td>Verifies connectivity after a device configuration is received</td>
</tr>
<tr>
<td>neighbor-inactivity-timeout</td>
<td>Configures a neighbor inactivity timeout</td>
</tr>
<tr>
<td>neighbor-info-interval</td>
<td>Configures the neighbor information exchange interval</td>
</tr>
<tr>
<td>noc</td>
<td>Configures NOC settings</td>
</tr>
<tr>
<td>ntp</td>
<td>Configure the NTP server settings</td>
</tr>
<tr>
<td>override-wlan</td>
<td>Configures WLAN RF Domain level overrides</td>
</tr>
<tr>
<td>power-config</td>
<td>Configures power mode features</td>
</tr>
<tr>
<td>preferred-controller-group</td>
<td>Specifies the group the system prefers for adoption</td>
</tr>
<tr>
<td>preferred-tunnel-controller</td>
<td>Configures the tunnel preferred by the system for tunneling extended VLAN traffic</td>
</tr>
<tr>
<td>radius</td>
<td>Configures device-level RADIUS authentication parameters</td>
</tr>
<tr>
<td>remove-override</td>
<td>Removes device overrides</td>
</tr>
<tr>
<td>rf-domain-manager</td>
<td>Enables the RF Domain manager</td>
</tr>
<tr>
<td>router</td>
<td>Configures dynamic router protocol settings</td>
</tr>
<tr>
<td>rsa-key</td>
<td>Assigns a RSA key to SSH</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>sensor-server</td>
<td>Configures an AirDefense sensor server</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Enables spanning tree commands</td>
</tr>
<tr>
<td>timezone</td>
<td>Configures time zone settings</td>
</tr>
<tr>
<td>trustpoint</td>
<td>Assigns a trustpoint to a service</td>
</tr>
<tr>
<td>tunnel-controller</td>
<td>Configures the tunneled WLAN (extended VLAN) wireless controller or service platform’s name</td>
</tr>
<tr>
<td>use</td>
<td>Defines the settings used by this feature</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configures VRRP group settings</td>
</tr>
<tr>
<td>wep-shared-key-auth</td>
<td>Enables support for 802.11 WEP shared key authentication</td>
</tr>
</tbody>
</table>
### 7.2.15 override-wlan

**Device Config Commands**

Configures WLAN RF Domain level overrides

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

override-wlan <WLAN> [ssid|vlan-pool|wpa-wpa2-psk]
override-wlan <WLAN> [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>} | wpa-wpa2-psk <WORD>]

**Parameters**

- **override-wlan WLAN** [ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>} | wpa-wpa2-psk <WORD>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WLAN&gt;</td>
<td>Specify the WLAN name. Configure the following WLAN parameters: SSID, VLAN pool, and WPA-WPA2 key.</td>
</tr>
<tr>
<td>SSID &lt;SSID&gt;</td>
<td>Configures the WLAN Service Set Identifier (SSID)</td>
</tr>
<tr>
<td>vlan-pool &lt;1-4094&gt; {limit &lt;0-8192&gt;}</td>
<td>Configures a pool of VLANs for the selected WLAN</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>
</tr>
</tbody>
</table>

**Examples**

rfs7000-00496-4A-A7-08(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 Block3B
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 5.4TestAP
neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

**Related Commands**

- **no** Removes RF Domain level WLAN overrides
7.2.16 remove-override

- **Device Config Commands**

Removes device overrides

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
remove-override <PARAMETERS>
```

Parameters

None

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
alias                                Alias
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
autoinstall                           Autoinstall settings
bridge                                Bridge group commands
captive-portal                        Captive portal
cdp                                    Cisco Discovery Protocol
channel-list                          Configure a channel list to be
advertised to wireless clients
cluster                                Cluster configuration
configuration-persistence             Automatic write of startup
configuration file                    configuration file
contact                                The contact
controller                            WLAN controller configuration
country-code                          The country of operation
critical-resource                     Critical Resource
crypto                                 Encryption related commands
device-upgrade                        Device firmware upgrade
dot1x                                  802.1X
dscp-mapping                          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
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)
l2tpv3                                 L2tpv3 protocol
l3e-lite-table                        L3e lite Table
led                                    LED on the device
lldp                                    Link Layer Discovery Protocol
```
location
logging
mac-address-table
mac-auth
memory-profile
mint
noc
ntp
override-wlan
power-config
preferred-controller-group
preferred-tunnel-controller
rf-domain-manager
router
routing-policy
sensor-server
spanning-tree
timezone
tunnel-controller
use
vrrp
service

ci

tst

tn

tf
	rr

rfs4000-229D58(config-device-00-23-68-22-9D-58)#
### 7.2.17 rsa-key

**Device Config Commands**

Assigns a RSA key to a device

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
rsa-key ssh <RSA-KEY-NAME>
```

**Parameters**

- `rsa-key ssh <RSA-KEY-NAME>`

<table>
<thead>
<tr>
<th><strong>rsa-key ssh &lt;RSA-KEY-NAME&gt;</strong></th>
<th>Assigns RSA key to SSH</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RSA-KEY-NAME&gt;</code></td>
<td>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 aplicenseley@1234 aplicensekey@123
rsa-key ssh rsa-key1
location Block3B
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 5.4TestAP
neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

```
no
```
Removes RSA key from service
7.2.18 sensor-server

Device Config Commands

Configures an AirDefense sensor server

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}  

Parameters

- sensor-server <1-3> ip <IP> {port [443|8443|<1-65535>]}  

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3&gt;</td>
<td>Selects a sensor server to configure</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Configures sensor server's IP address</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>Optional. Configures the port. The options are:</td>
</tr>
<tr>
<td></td>
<td>- 443 – The default port used by the AirDefense server</td>
</tr>
<tr>
<td></td>
<td>- 8443 – The default port used by advanced WIPS</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-65535&gt; – Manually sets the port number of the advanced WIPS/AirDefense server</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  

Related Commands

- no  
  Removes configured sensor server
### 7.2.19 timezone

**Device Config Commands**

Configures device's timezone

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

timezone <TIMEZONE>

**Parameters**

- timezone <TIMEZONE>

**Examples**

```bash
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 Block3B
  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 5.4TestAP
  neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

- `no` | Removes device's configured timezone
7.2.20 trustpoint

Device Config Commands

Assigns a trustpoint

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

trustpoint [https|radius-ca|radius-server] <TRUSTPOINT>

Parameters

- trustpoint [https|radius-ca|radius-server] <TRUSTPOINT>

<table>
<thead>
<tr>
<th>https &lt;TRUSTPOINT&gt;</th>
<th>Assigns a specified trustpoint to HTTPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TRUSTPOINT&gt; – Specify the trustpoint name.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>radius-ca &lt;TRUSTPOINT&gt;</th>
<th>Assigns a trustpoint as a certificate authority for validating client certificates in EAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TRUSTPOINT&gt; – Specify the trustpoint name.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>radius-server &lt;TRUSTPOINT&gt;</th>
<th>Specifies the name of the trustpoint. Install the trustpoint using PKI commands in the enable mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TRUSTPOINT&gt; – Specify the trustpoint name.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

```plaintext
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#trustpoint radius-ca trust2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
```

Related Commands

- no

Removes configured trustpoint from service
7.2.21 mirror

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:

- Service Platforms — NX4524, NX6524

NOTE: Port mirroring is not supported on NX4500 or NX6500 models, as they only support GE ports 1 - 2. Additionally, port mirroring is not supported on uplink (up) ports or wired ports on any controller or service platform model.

Syntax

```
```

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.

| to interface [INTERFACE-NAME]|ge <1-24>] | Selects the GE port used as the port destination to span packets from the selected source. Use one of the following options to identify the destination port:
| | • <INTERFACE-NAME> – Specifies the destination port name
| | • ge <1-24> – Specifies the destination GE port index
| | The destination port serves as a duplicate image of the source port and can be used to send packets to a network diagnostic without disrupting the behavior on the original port. The destination port transmits only mirrored traffic and does not forward received traffic. Additionally, address learning is disabled on the destination port. The destination port is also referred to as the Mirror-to-Port (MTP).

| direction [any|inbound|outbound] | Optional. Defines the direction data packets are spanned from the selected source to the defined destination. The packets spanned from the selected source to the destination depend on whether Inbound, Outbound or Any is selected as the direction.
| | • any – Spans packets in either direction (inbound and outbound)
| | • inbound – Spans received packets only
| | • outbound – Spans transmitted packets only
Usage Guidelines
All mirroring sessions must use the same destination port for packet capture.

Examples
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
- Session - Source - Destination - Direction -
  1 - ge3 - ge24 - any
  2 - ge7 - ge24 - inbound
  3 - ge5 - ge24 - outbound

nx4524-470984#

Related Commands

no | Disables data packets mirroring on GE ports
**7.2.22 raid**

*Device Config Commands*

Enables/disables RAID alarms

For more information on RAID, see `raid`.

Supported in the following platforms:

- Service Platforms — NX9500, NX75XX

**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)#

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 ge1
    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 |
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`: 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-policy-test)#
```
8.1 aaa-policy

Table 8.1 summarizes AAA policy configuration 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 8-22</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 8-23</td>
</tr>
<tr>
<td>use</td>
<td>Defines the AAA command settings</td>
<td>page 8-24</td>
</tr>
</tbody>
</table>
### 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
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> secret [0 <SECRET>|2 <SECRET>|<SECRET>]
{port <1-65535>}
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT>
{strip}
accounting server <1-6> onboard [self|controller]
accounting server <1-6> proxy-mode [none|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**
    - **interval <60-3000>**
      - Configures the interim accounting interval
      - Specify the interim interval from 60 - 3600 seconds. The default is 1800 seconds.

- **accounting server preference [auth-server-host|auth-server-number|none]**
  - **server**
    - **preference**
      - Configures a RADIUS accounting server’s settings
      - 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 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>
<tbody>
<tr>
<td>dscp &lt;0-63&gt;</td>
<td>Sets the Differentiated Services Code Point (DSCP) value for Quality of Service (QOS) monitoring. This value is used in generated RADIUS packets.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-63&gt; – Sets the DSCP value from 0 - 63</td>
</tr>
<tr>
<td>retry-timeout-factor &lt;50-200&gt;</td>
<td>Sets the scaling factor for retransmission timeouts. The timeout at each attempt is a function of this retry-timeout factor and the attempt number.</td>
</tr>
<tr>
<td></td>
<td>• &lt;50-200&gt; – Specify a value from 50 - 200. The default is 100.</td>
</tr>
<tr>
<td></td>
<td>If the scaling factor is 100, the interval between two consecutive retries remains the same, irrespective of the number of retries.</td>
</tr>
<tr>
<td></td>
<td>If the scaling factor is less than 100, the interval between two consecutive retries reduces with subsequent retries.</td>
</tr>
<tr>
<td></td>
<td>If this scaling factor is greater than 100, the interval between two consecutive retries increases with subsequent retries.</td>
</tr>
</tbody>
</table>

• accounting server <1-6> host <IP/HOSTNAME> 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>
<tbody>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Configures the accounting server’s hostname or IP address</td>
</tr>
<tr>
<td>secret [0 &lt;SECRET&gt;</td>
<td>2 &lt;SECRET&gt;</td>
</tr>
<tr>
<td></td>
<td>• 0 &lt;SECRET&gt; – Configures a clear text secret key</td>
</tr>
<tr>
<td></td>
<td>• 2 &lt;SECRET&gt; – Configures an encrypted secret key</td>
</tr>
<tr>
<td></td>
<td>• &lt;SECRET&gt; – Specify the secret key. This shared secret should not exceed 127 characters.</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Configures the accounting server’s UDP port (the port used to connect to the accounting server)</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Sets the port number from 1 - 65535 (default port is 1813)</td>
</tr>
</tbody>
</table>

• 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>
<tbody>
<tr>
<td>nai-routing</td>
<td>Enables Network Access Identifier (NAI) routing</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>realm-type</td>
<td>Selects the match type used on the username</td>
</tr>
</tbody>
</table>
### Accounting Server Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **prefix|suffix** | Select one of the following options:  
  - *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`) |
| **realm** | 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.  
  - `<REALM-TEXT>` – Specifies the matching text including the delimiter (a delimiter is typically `'` or `@`) |
| **strip** | Optional. Strips the realm from the username before forwarding the request to the RADIUS server |

#### Accounting Server Command Reference

- **server <1-6> onboard [self|controller]**  
  
- **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.**  
  
- **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-controller|through-mint-host <HOSTNAME/MINT-ID>|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.**  
  
- **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>}**  
  
- **server <1-6> 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.**  
  
- **attempts <1-10>**  
  
- **Optional. Specifies the number of times a transmission request is attempted.**  
  
- **<1-10> – Specify a value from 1 - 10.**
• **accounting type [start-interim-stop|start-stop|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**

```
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 company 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
accounting server 2 host 172.16.10.10 secret 0 company 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX6500, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa|framed-mtu<location-information|nas-ipv6-address|operator-name|service-type]
```

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acct-delay-time</td>
<td>Enables support for <em>accounting-delay-time</em> 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. <strong>Note:</strong> Including the <em>acct-delay-time</em> 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.</td>
</tr>
<tr>
<td>acct-multi-session-id</td>
<td>Enables support for <em>accounting-multi-session-id</em> 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.</td>
</tr>
<tr>
<td>chargeable-user-identity</td>
<td>Enables support for <em>chargeable-user-identity</em> attribute.</td>
</tr>
</tbody>
</table>
### AAA-POLICY 8 - 9

- **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-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.

- **attribute location-information [include-always|none|server-requested]**

  **location-information [include-always|none|server-requested]**

  Enables/disables 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
  - **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

  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 <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.

  - **<OPERATOR-NAME>** – Specify the network operator’s name.
### attribute service-type [framed|login]

| service-type [framed|login] | 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 – 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. |
|                            | • 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
     accounting server 2 host 172.16.10.10 secret 0 company 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-test1)#
```

### Related Commands

<table>
<thead>
<tr>
<th>no</th>
<th>Resets values or disables commands</th>
</tr>
</thead>
</table>
### 8.1.3 authentication

- **aaa-policy**

Configures user authentication parameters

Supported in the following platforms:

- Access Points — AP300, 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, 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]

 authentication server <1-6> dscp <0-63>

 authentication server <1-6> host <IP/HOSTNAME> 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 [controller|self]

 authentication server <1-6> proxy-mode [none|through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]

 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>|identity-request-retry-timeout <10-5000>|identity-request-timeout <1-60>|retry-timeout-factor <50-200>|timeout <1-60>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap</td>
<td>Configures EAP authentication parameters</td>
</tr>
<tr>
<td>wireless-client</td>
<td>Configures wireless client’s EAP parameters</td>
</tr>
</tbody>
</table>
| 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. |
| 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 3 seconds. |
### retry-timeout-factor
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;50-200&gt;</td>
<td>Configures the spacing between successive EAP retries</td>
</tr>
<tr>
<td></td>
<td>- &lt;50-200&gt; – Specify a value from 50 - 200. The default is 100.</td>
</tr>
<tr>
<td></td>
<td>A value of 100 indicates the interval between two consecutive retries remains the same irrespective of the number of retries.</td>
</tr>
<tr>
<td></td>
<td>A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry.</td>
</tr>
<tr>
<td></td>
<td>A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.</td>
</tr>
</tbody>
</table>

### timeout
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-60&gt;</td>
<td>Configures the interval, in seconds, between successive EAP-identity request sent to a wireless client</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-60&gt; – Specify a value from 1 - 60 seconds.</td>
</tr>
</tbody>
</table>

### authentication protocol
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[chap</td>
<td>mschap</td>
</tr>
<tr>
<td></td>
<td>- chap – Uses Challenge Handshake Authentication Protocol (CHAP)</td>
</tr>
<tr>
<td></td>
<td>- mschap – Uses Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)</td>
</tr>
<tr>
<td></td>
<td>- mschapv2 – Uses MS-CHAP version 2</td>
</tr>
<tr>
<td></td>
<td>- pap – Uses Password Authentication Protocol (PAP) (default authentication protocol used)</td>
</tr>
</tbody>
</table>

### server
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-6&gt;</td>
<td>Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</td>
</tr>
</tbody>
</table>

### dscp
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-63&gt;</td>
<td>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. The default is 46.</td>
</tr>
</tbody>
</table>

### server
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-6&gt;</td>
<td>Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</td>
</tr>
</tbody>
</table>

### host
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/HOSTNAME&gt;</td>
<td>Sets the RADIUS authentication server’s IP/alias address or hostname. The host alias IP or host alias name must be an existing one.</td>
</tr>
</tbody>
</table>

### secret
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0 &lt;SECRET&gt;</td>
<td>2 &lt;SECRET&gt;</td>
</tr>
<tr>
<td></td>
<td>- 0 &lt;SECRET&gt; – Configures a clear text secret</td>
</tr>
<tr>
<td></td>
<td>- 2 &lt;SECRET&gt; – Configures an encrypted secret</td>
</tr>
<tr>
<td></td>
<td>- &lt;SECRET&gt; – Specify the secret key. The shared key should not exceed 127 characters.</td>
</tr>
</tbody>
</table>

### port
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Optional. Specifies the RADIUS authentication server’s UDP port (this port is used to connect to the RADIUS server)</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-65535&gt; – Specify a value from 1 - 65535. The default port is 1812.</td>
</tr>
</tbody>
</table>
### AAA-POLICY 8 - 13

#### authentication server <1-6> nac

| 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. |

#### 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.  
|              | • <1-6> – Specifies the RADIUS server index from 1 - 6. |

#### nai-routing

Enables NAI routing. When enabled, AAA servers identify clients using NAI.

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]

Confirms 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 50 characters. 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:
- Prefix - 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.
### authentication server <1-6> onboard [controller|self]

| 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>

| onboard [controller|self] | Selects the onboard RADIUS server for authentication instead of an external host  
| --- | --- |
| 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-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.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-6&gt; – Sets the RADIUS server index between 1 - 6</td>
<td></td>
</tr>
</tbody>
</table>

| proxy-mode [none|through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager] | Configures the mode for proxying a request  
| --- | --- |
| none – Proxying is not done. The packets are sent directly using the IP address of the device.  
| 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.  
<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>

| 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.  
| 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.  
<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>

| 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.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-60&gt; – Specify a value from 1 - 60 seconds. The default is 3 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

| attempts <1-10> | Optional. Indicates the number of retry attempts to make before giving up  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-10&gt; – Specify a value from 1 - 10. The default is 3.</td>
<td></td>
</tr>
</tbody>
</table>
Examples

rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 host 172.16.10.10 secret company port 1009

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 company port 1009
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 company 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets authentication parameters on this AAA policy</td>
</tr>
</tbody>
</table>
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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
health-check interval <60-86400>
```

**Parameters**

- `health-check interval <60-86400>`

<table>
<thead>
<tr>
<th>interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&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>&lt;60-86400&gt;</td>
<td>Specify a value from 60 - 86400 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 company port 1009
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 company 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**

- `no` Resets the health-check interval for AAA servers
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
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 AABBCC-DDEEFF</td>
</tr>
<tr>
<td>no-delim</td>
<td>Configures the MAC address format as AABBCCDDDEEFF (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.CC:DD:EE:FF</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</td>
<td>Configures RADIUS attributes to which this MAC format is applicable</td>
</tr>
<tr>
<td>[all]</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>username-password</td>
<td>• username-password – Applies only to the username and password fields (default setting)</td>
</tr>
</tbody>
</table>

**Examples**

```
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 company port 1009
    authentication server 5 timeout 10
    accounting server 2 host 172.16.10.10 secret 0 company 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Resets the MAC address format to default (pair-hyphen)</td>
</tr>
</tbody>
</table>
### 8.1.6 no

Negates a AAA policy command or sets its default

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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-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 accounting interim interval**
  - Disables the periodic submission of accounting information

- **no accounting server preference**
  - Resets the accounting server’s preference to default

- **no accounting server <1-6> {dscp|nai-routing|proxy-mode|retry-timeout-factor|
   timeout}**
  - Resets the RADIUS accounting server’s (identified by its index number) settings

- **dscp**
  - Optional. Resets the DSCP value for RADIUS accounting
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nai-routing</td>
<td>Optional. Disables NAI forwarding requests</td>
</tr>
<tr>
<td>proxy-mode</td>
<td>Optional. Resets proxy mode to the default of “no proxying”</td>
</tr>
<tr>
<td>retry-timeout-factor</td>
<td>Optional. Resets retry timeout to its default of 100</td>
</tr>
<tr>
<td>timeout</td>
<td>Optional. Resets access parameters, such as timeout values and retry attempts to their default</td>
</tr>
</tbody>
</table>

- **no accounting type**

  - no accounting type
    - Resets the type of RADIUS accounting packets generated, to its default (start/stop)

- **no attribute** [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa audit-session-id|framed-mtu|location-information|nas-ipv6-address|operator-name|service-type]

  - no attribute acct-delay-time
    - Disables support for accounting-delay-time attribute in accounting requests
  - no attribute acct-multi-session-id
    - Disables support for accounting-multi-session-id attribute
  - no attribute chargeable-user-identity
    - Disables support for chargeable-user-identity attribute
  - no attribute cisco-vsa audit-session-id
    - Removes the configured CISCO VSA audit session ID
  - no attribute framed-mtu
    - Resets Framed-MTU RADIUS server attribute in access and accounting requests
  - no attribute location-information
    - Disables support for RFC5580 location information attribute
  - no attribute nas-ipv6-address
    - Disables support for the NAS IPv6 address attribute
  - no attribute service-type
    - Disables support for the service-type (6) attribute

- **no authentication protocol**

  - no authentication eap wireless-client [attempts|identity-request-timeout| retry-timeout-factor|timeout]

  - no authentication eap wireless-client
    - Resets EAP parameters for wireless clients
  - attempts
    - Resets the number of times a RADIUS request is sent to a wireless client to default (3)
  - identity-request-retry-timeout
    - Resets the interval after which an EAP-identity request to the wireless client is retried
  - identity-request-timeout
    - Resets EAP identity request timeout to its default
  - retry-timeout-factor
    - Resets EAP retry timeout to its default of 100
  - timeout
    - Resets EAP timeout to its default

- **no authentication protocol**

  - authentication protocol
    - Resets the authentication protocol used for non-EAP authentication to its default (PAP authentication)
no authentication server <1-6> {dscp|nac|nai-routing|proxy-mode|retry-timeout-factor|timeout}

- **no authentication server**<1-6> | Resets the RADIUS authentication server’s (identified by its index number) settings
- **dscp** | Optional. Resets the DSCP value for RADIUS authentication
- **nac** | Optional. Disables NAC on the selected RADIUS authentication server
- **nai-routing** | Optional. Disables NAI forwarding requests
- **proxy-mode** | Optional. Resets proxy mode to the default of “no proxying”
- **retry-timeout-factor** | Optional. Resets retry timeout to its default of 100
- **timeout** | Optional. Resets all access parameters, such as timeout and retry attempts to their default

no health-check interval

- **no health-check interval** | Resets all RADIUS servers’ health check interval to its default

no mac-address-format

- **no mac-address format** | Resets the MAC address format used in RADIUS request frames

no proxy-attribute [nas-identifier|nas-ip-address]

- **no proxy-attribute** [nas-identifier|nas-ip-address] | Resets RADIUS attribute behavior when proxying through a controller or RF Domain manager

no server-pooling-mode

- **no server-pooling-mode** | Resets the mode used to select a AAA server from a pool of configured servers

no use nac-list

- **no use nac-list** | Detaches the current NAC list from this AAA policy

**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 company port 1009
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 company 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)#
```

```
rfs7000-37FABE(config-aaa-policy-test)#no accounting server 2 timeout 2
rfs7000-37FABE(config-aaa-policy-test)#no accounting interim interval
rfs7000-37FABE(config-aaa-policy-test)#no health-check interval
rfs7000-37FABE(config-aaa-policy-test)#no attribute framed-mtu
rfs7000-37FABE(config-aaa-policy-test)#no authentication protocol
```
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 company port 1009
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 company 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)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Configures RADIUS accounting parameters</td>
</tr>
<tr>
<td>attribute</td>
<td>Configures RADIUS Framed-MTU attribute used in access and accounting requests.</td>
</tr>
<tr>
<td>authentication</td>
<td>Configures RADIUS authentication parameters</td>
</tr>
<tr>
<td>health-check</td>
<td>Configures health-check parameters</td>
</tr>
<tr>
<td>mac-address-format</td>
<td>Configures the MAC address format used in RADIUS packets</td>
</tr>
<tr>
<td>proxy-attribute</td>
<td>Configures RADIUS server’s attribute behavior when proxying through a wireless controller or a RF Domain Manager</td>
</tr>
<tr>
<td>server-pooling-mode</td>
<td>Configures the RADIUS server pooling mode</td>
</tr>
<tr>
<td>use</td>
<td>Permits the use of NAC access lists</td>
</tr>
</tbody>
</table>
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 — AP300, 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, 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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas-identifier [originator</td>
<td>proxier]</td>
</tr>
<tr>
<td></td>
<td>• originator – Configures the NAS identifier as the originator of the RADIUS request. The originator could be an AP, or a wireless controller with radio.</td>
</tr>
<tr>
<td></td>
<td>• proxier – Configures the proxying device as the NAS identifier. The device could be a controller or a RF Domain manager.</td>
</tr>
<tr>
<td>nas-ip-address [none</td>
<td>proxier]</td>
</tr>
<tr>
<td></td>
<td>• none – NAS IP address attribute is not filled</td>
</tr>
<tr>
<td></td>
<td>• proxier – NAS IP address is filled by the proxying device. The device could be a controller or a RF Domain manager.</td>
</tr>
</tbody>
</table>

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

- **aaa-policy**

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`server-pooling-mode [failover|load-balance]`

**Parameters**

- `server-pooling-mode [failover|load-balance]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>failover</td>
<td>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.</td>
</tr>
<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 company port 1009
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 company 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

use nac-list <NAC-LIST-NAME>

Parameters

- use nac-list <NAC-LIST-NAME>

<table>
<thead>
<tr>
<th>nac-list</th>
<th>Associates a NAC list with this AAA policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NAC-LIST-NAME&gt;</td>
<td>- &lt;NAC-LIST-NAME&gt; — Specify the NAC list name (should be existing and configured).</td>
</tr>
</tbody>
</table>

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 company port 1009
  authentication server 5 timeout 10
  accounting server 2 host 172.16.10.10 secret 0 company 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

| no | Resets set values or disables commands |
| nac-list | Creates a NAC list |
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 ‘adoptee’. 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 controller.

---

**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>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RFS7000</td>
<td>NX7500</td>
<td>NX9000</td>
<td>NX9XXX (NX9500 &amp; NX9510)</td>
</tr>
<tr>
<td>RFS4000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RFS6000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RFS7000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NX45XX</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NX65XX</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NX7500</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NX9000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>NX9XXX</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</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>
```

```
rfs7000-37PABE(config)#auto-provisioning-policy test
rfs7000-37PABE(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
- **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)#
## 9.1 auto-provisioning-policy

Table 9.1 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 9-11</td>
</tr>
<tr>
<td>deny</td>
<td>Adds a deny adoption rule</td>
<td>page 9-12</td>
</tr>
<tr>
<td>evaluate-always</td>
<td>Sets the flag to evaluate the policy everytime</td>
<td>page 9-15</td>
</tr>
<tr>
<td>redirect</td>
<td>Adds a rule redirecting device adoption to a specified controller within the system</td>
<td>page 9-16</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>
### 9.1.1 adopt

**auto-provisioning-policy**

Adds device adoption rules

Supported in the following platforms:

- Access Points — ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopt [ap621</td>
<td>ap622</td>
</tr>
<tr>
<td>adopt [ap621</td>
<td>ap622</td>
</tr>
<tr>
<td>adopt [ap621</td>
<td>ap622</td>
</tr>
<tr>
<td>adopt [ap621</td>
<td>ap622</td>
</tr>
</tbody>
</table>

**Parameters**

- adopt [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap6532|ap6562|ap71xx|ap7502| ap7522|ap7532|ap81xx|ap82xx|rf54000|rf56000|rf7000|nx45xx|nx65xx|nx75xx|nx9000] precedence <1-10000> [profile|rf-domain] <LOCATION-SUBSTRING> dhcp-option <DHCP-OPTION> [fqdn <FQDN>|ip <START-IP>|<END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING> | Concurrently defines adoption device rules. The rule applies to the selected device types. Specify the device type, the rule, and assign the precedence to the rule. |
### 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'

**Available tokens:**

- `$FQDN` - references FQDN of adopting device
- `$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

### 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]'

**Available tokens:**

- `$FQDN` - references FQDN of adopting device
- `$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

**Available built-in aliases:**

- `_builtin_rf-domain` - rf-domain of adopting device

**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 $DOMAIN test.company.com'. In this example, the string-alias `$DOMAIN` is mapped to the string: `test.company.com`. For more information, see alias.

### any

Indicates any device. Any device seeking adoption is adopted.
| **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: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX75XX, and NX9000. |
| **precedence** | Sets the rule precedence. A rule with a lower value has a higher precedence. <1-10000> |
| **profile** | 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-$MODEL[1:6]', 'FQDN[1:4]-indoor'. Available tokens: |
| `$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 |
### 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 an alias. Or a template with appropriate substitution tokens, such as `$CDP[1:7]`, `$DNS-SUFFIX[1:5]`

Available tokens:

- `$FQDN` - references FQDN of adopting device
- `$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

Available built-in aliases: `_builtin_rf-domain` - rf-domain of adopting device

**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 $DOMAIN test.company.com’. In this example, the string-alias `$DOMAIN` is mapped to the string: `test.company.com`. For more information, see `alias`.

### cdp-match

**<LOCATION-SUBSTRING>**

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.

- `<LOCATION-SUBSTRING>` – Specify the value to match. Devices matching the specified value are adopted.

### dhcp-option

**<DHCP-OPTION>**

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.

- `<DHCP-OPTION>` – Specify the DHCP option. Devices matching the specified value are adopted.

### fqdn <FQDN>

Matches a substring to the **Fully Qualified Domain Name (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. This parameter allows a device to adopt based on its FQDN value.

- `<FQDN>` – Specify the FQDN. Devices matching the specified value are adopted.

### ip

**[<START-IP> <END-IP> | <IP/MASK>]**

Adopts a device if its IP address matches the specified IP address or is within the specified IP address range. Or if the device is a part of the specified subnet.

- `<START-IP>` – Specify the first IP address in the range.
- `<END-IP>` – Specify the last IP address in the range.
- `<IP/MASK>` – Specify the IP subnet and mask to match against the device's IP address.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>lldp-match</strong></td>
<td>Matches a substring in a list of <em>Link Layer Discovery Protocol</em> (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>
<tr>
<td><strong>mac</strong></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><code>&lt;START-MAC&gt;</code></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><code>{&lt;END-MAC&gt;}</code></td>
<td>- <code>&lt;END-MAC&gt;</code> – Optional. Specify the last MAC address in the range.</td>
</tr>
<tr>
<td>model-number</td>
<td>Adopts a device if its model number matches <code>&lt;MODEL-NUMBER&gt;</code></td>
</tr>
<tr>
<td><code>&lt;MODEL-NUMBER&gt;</code></td>
<td>- <code>&lt;MODEL-NUMBER&gt;</code> – Specify the model number.</td>
</tr>
<tr>
<td>rf-domain</td>
<td>Adopts a device if its RF Domain matches <code>&lt;RF-DOMAIN-NAME&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RF-DOMAIN-NAME&gt;</code></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. 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><strong>Available tokens:</strong></td>
</tr>
<tr>
<td><code>$FQDN</code></td>
<td>- references FQDN of adopting device</td>
</tr>
<tr>
<td><code>$CDP</code></td>
<td>- references CDP Device Id of wired switch to which adopting device is connected</td>
</tr>
<tr>
<td><code>$LLDP</code></td>
<td>- references LLDP System Name of wired switch to which adopting device is connected</td>
</tr>
<tr>
<td><code>$DHCP</code></td>
<td>- references DHCP Option Value received by the adopting device</td>
</tr>
<tr>
<td><code>$SN</code></td>
<td>- references SERIAL NUMBER of adopting device</td>
</tr>
<tr>
<td><code>$MODEL</code></td>
<td>- references MODEL NUMBER of adopting device</td>
</tr>
<tr>
<td><code>$DNS-SUFFIX</code></td>
<td>- references FQDN excluding the hostname of the adopting device</td>
</tr>
<tr>
<td></td>
<td><strong>Available built-in aliases:</strong></td>
</tr>
<tr>
<td></td>
<td><code>_builtin_rf-domain</code> - rf-domain of adopting device</td>
</tr>
<tr>
<td>Note:</td>
<td><strong>Note:</strong> Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, ‘alias string <code>$DOMAIN</code> test.company.com’. In this example, the string-alias <code>$DOMAIN</code> is mapped to the string: <code>test.company.com</code>. For more information, see <code>alias</code>.</td>
</tr>
<tr>
<td>serial-number</td>
<td>Adopts a device if its serial number matches <code>&lt;SERIAL-NUMBER&gt;</code></td>
</tr>
<tr>
<td><code>&lt;SERIAL-NUMBER&gt;</code></td>
<td>- <code>&lt;SERIAL-NUMBER&gt;</code> – Specify the serial number.</td>
</tr>
<tr>
<td>vlan <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>
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

<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>ap81xx-711728</td>
<td>B4-C7-99-71-17-28</td>
<td>default-ap81xx</td>
<td>default</td>
<td>00-23-68-22-9D-58</td>
</tr>
<tr>
<td>2</td>
<td>rfs4000-229D58</td>
<td>00-23-68-22-9D-58</td>
<td>default-rfs4000</td>
<td>default</td>
<td></td>
</tr>
</tbody>
</table>

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 adopt rule</td>
</tr>
</tbody>
</table>
9.1.2 default-adoption

Adopts devices, even when no matching rules are defined. Assigns a default profile and default RF Domain.

Supported in the following platforms:

- Access Points — ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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
  adopt ap81xx precedence 1 profile default-ap81xx vlan 1
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 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 — ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
deny [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000] nx45xx
```  

```plaintext
deny [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000] nx45xx
```  

```plaintext
deny [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000] nx45xx
```  

```plaintext
deny [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000] nx45xx
```  

**Parameters**

- **deny [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000] nx45xx**

  **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: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX75XX, and NX9000 series.

  **precedence <1-10000> any**

  **precedence <1-10000>** 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.

- **deny [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502] nx45xx**

  **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: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX75XX, and NX9000.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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)</td>
</tr>
<tr>
<td>ip [START-IP] END-IP</td>
<td>Denies adoption if a device’s IP address matches the specified IP address or is within the specified IP address range</td>
</tr>
<tr>
<td>lldp-match &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.</td>
</tr>
<tr>
<td>mac &lt;START-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</td>
</tr>
<tr>
<td>model-number &lt;MODEL-NUMBER&gt;</td>
<td>Denies adoption if a device’s model number matches &lt;MODEL-NUMBER&gt;</td>
</tr>
<tr>
<td>serial-number &lt;SERIAL-NUMBER&gt;</td>
<td>Denies adoption if a device’s serial number matches &lt;SERIAL-NUMBER&gt;</td>
</tr>
</tbody>
</table>
### Examples

```bash
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><code>no</code></td>
<td>Removes a deny adoption rule</td>
</tr>
</tbody>
</table>
9.1.4 evaluate-always

- auto-provisioning-policy

Sets the flag to evaluate the policy everytime irrespective of previous adoption status

Supported in the following platforms:

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

Syntax
evaluate-always

Parameters
None

Examples
rfs6000-81742D(config-auto-provisioning-policy-test)#evaluate-always
rfs6000-81742D(config-auto-provisioning-policy-test)#
## 9.1.5 redirect

A rule is added redirecting device adoption to another controller within the system. Devices seeking adoption are redirected to a specified controller based on the redirection parameters specified.

Supported in the following platforms:

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

### Syntax

```
redirect [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]
redirect [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]
precedence <1-10000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>]
```

### Parameters

- **redirect [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|
ap7522|ap7532|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]
  - Sets the rule precedence. Rules with lower values get precedence over rules with higher values.

- **controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>]
  - 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

- **any**
  - Indicates any device. Any device seeking adoption is redirected.

---

**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`.
### AUTO-PROVISIONING-POLICY 9 - 17

- **deny** [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap81xx|ap82xx|rf64000|rf6000|rf7000|nx45xx|nx65xx|nx75xx|nx9000]  
  precedence <1-1000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-MAC>{<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]  

- **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 type options are: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP5131, AP6562, AP71XX, AP81XX, AP7502, AP7522, AP7532, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX75XX, and NX9000.  
  **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.

#### controller [<CONTROLLER-IP>|
  <CONTROLLER-HOSTNAME>] 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  
  After specifying the rule precedence and the controller, specify the match criteria.

#### 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 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.

#### ip [<START-IP> 
  <END-IP>|<IP/MASK>] Configures a range of IP addresses and subnet address. Devices having IP addresses within the specified range or are part of the specified subnet are redirected.  
  - <START-IP> – Specify the first IP address in the range.  
  - <END-IP> – Specify the last IP address in the range.  
  - <IP/MASK> – Specify the IP 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.
Examples

```bash
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 4
```

```bash
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 5
ccontroller 192.168.13.10 model-number AP-8132-66040-US
```

```bash
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
```

Related Commands

```bash
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 — ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|ap82xx|
        rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000]

upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|ap82xx|
        rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] precedence <1-10000> |
        [any|cdp-match|dhcp-option|fqdn|ip|lldp-match|mac|model-number|serial-number|vlan]

upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|ap82xx|
        rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] precedence <1-10000> any

upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|ap82xx|
        rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] precedence <1-10000> |
        [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>| 
         ip [<START-IP> <END-IP>|<IP/MASK>|lldp-match <LLDP-STRING>| 
         mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>| 
         serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]|lldp-match <LLDP-STRING>| 
         mac <STARTING-MAC> {<ENDING-MAC>}/model-number <MODEL-NUMBER>| 
         serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

**Parameters**

- **upgrade [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|
  ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] precedence <1-10000> any**

<table>
<thead>
<tr>
<th>upgrade</th>
<th>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: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX75XX, and NX9000 series.</th>
</tr>
</thead>
<tbody>
<tr>
<td>precedence</td>
<td>Sets the rule precedence. Rules with lower values get precedence over rules with higher values.</td>
</tr>
<tr>
<td>any</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>
**upgrade** [ap621|ap622|ap650|ap6511|ap6521|ap6522|ap6532|ap6562|ap71xx|ap81xx|ap82xx|rfs4000|rfs6000|rfs7000|nx45xx|nx65xx|nx75xx|nx9000] precedence <1-10000> [cdp-match <LOCATION-SUBSTRING> dhcp-option <DHCP-OPTION> mac <START-MAC> {<END-MAC>} model-number <MODEL-NUMBER> serial-number <SERIAL-NUMBER> vlan <VLAN-ID>] lldp-match <LLDP-STRING> mac <STARTING-MAC> {<ENDING-MAC>} model-number <MODEL-NUMBER> serial-number <SERIAL-NUMBER> vlan <VLAN-ID>]

**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: AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX, RFS4000, RFS6000, RFS7000, NX45XX, NX65XX, NX75XX, and NX9000 series.

**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 IP addresses within the specified range or are part of the specified subnet are upgraded.
- <START-IP> – Specify the first IP address in the range.
- <END-IP> – Specify the last IP address in the range.
- <IP/MASK> – Specify the IP 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.

**mac** <START-MAC> {<END-MAC>} Configures a single or a range of MAC addresses. Devices matching the specified values are upgraded.
- <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 upgraded.
serial-number <SERIAL-NUMBER>

- Configures the device's serial number
  - <SERIAL-NUMBER> – Specify the serial number. Devices matching the specified serial number are upgraded.

vlan <VLAN-ID>

- Configures the VLAN ID
  - <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are upgraded.

Examples

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

no

- Removes an upgrade rule
**9.1.7 no**

- **auto-provisioning-policy**

Removes a deny, permit, or redirect rule from the specified auto provisioning policy

Supported in the following platforms:

- Access Points — ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510

**Syntax**

```
no [adopt|default-adoption|deny|redirect|upgrade]
no adopt precedence <1-10000>
no deny precedence <1-10000>
no default-adoption
no redirect precedence <1-10000>
no upgrade precedence <1-10000>
```

**Parameters**

- **no adopt precedence <1-10000>**

<table>
<thead>
<tr>
<th>adopt precedence &lt;1-10000&gt;</th>
<th>Removes the adoption rule identified by the specified precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• precedence &lt;1-10000&gt; – Specify the rule precedence.</td>
</tr>
</tbody>
</table>

- **no deny precedence <1-10000>**

<table>
<thead>
<tr>
<th>deny precedence &lt;1-10000&gt;</th>
<th>Removes the deny adoption rule identified by the specified precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• precedence &lt;1-10000&gt; – Specify the rule precedence.</td>
</tr>
</tbody>
</table>

- **no default-adoption**

| default-adoption | Removes the default adoption rule. When the default adoption rule is absent, devices not matching any of the configured deny or permit criteria are denied adoption |

- **no redirect precedence <1-10000>**

<table>
<thead>
<tr>
<th>redirect precedence &lt;1-10000&gt;</th>
<th>Removes the redirect adoption rule identified by the specified precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• precedence &lt;1-10000&gt; – Specify the rule precedence.</td>
</tr>
</tbody>
</table>

- **no upgrade precedence <1-10000>**

<table>
<thead>
<tr>
<th>upgrade precedence &lt;1-10000&gt;</th>
<th>Removes the device upgrade rule identified by the specified precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• precedence &lt;1-10000&gt; – Specify the rule precedence.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the auto-provisioning-policy 'test' settings before the 'no' commands are executed:

```bash
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 ap71xxx precedence 2 model-number AP7131N
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

```bash
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
```

The following example shows the auto-provisioning-policy 'test' settings after the 'no' commands are executed:

```bash
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
  adopt ap81xx precedence 1 rf-domain TechPubs vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

```bash
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)#
```

```bash
rfs4000-229D58(config-auto-provisioning-policy-test)#no upgrade precedence 1
```

The following example shows the auto-provisioning-policy 'test' settings after the 'no' commands are executed:

```bash
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)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopt</td>
<td>Configures an adoption rule</td>
</tr>
<tr>
<td>default-adoption</td>
<td>Configures the rule for adopting devices when adopt or deny rules are not defined</td>
</tr>
<tr>
<td>deny</td>
<td>Configures a deny adoption rule</td>
</tr>
<tr>
<td>redirect</td>
<td>Configures a rule redirecting devices seeking adoption to another controller</td>
</tr>
<tr>
<td>upgrade</td>
<td>Configures a rule for upgrade of adopted devices</td>
</tr>
</tbody>
</table>
CHAPTER 10
ASSOCIATION-ACL-POLICY

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 an 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.
### 10.1 association-acl-policy

Table 10.1 summarizes association ACL policy configuration 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 10-8</td>
</tr>
</tbody>
</table>
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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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>`
  - Adds a single device or a set of devices to the deny list
  - `<STARTING-MAC>`: 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.

- `deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>`
  - Adds a single device or a set of devices to the deny list
  - `<STARTING-MAC>`: To add a set of devices, provide the range of MAC addresses.
  - `<ENDING-MAC>`: Specify the first MAC address in the range.
  - `<precedence <1-1000>`: Sets a precedence rule. Rules are applied in an increasing order of precedence.
    - `<1-1000>` – Specify a 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**

```plaintext
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 — AP300, 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, 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

- deny <STARTING-MAC> precedence <1-1000>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no deny &lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>Removes a single device or a set of devices from the deny list</td>
</tr>
<tr>
<td>&lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>To remove a single device, enter its MAC address in the &lt;STARTING-MAC&gt; parameter.</td>
</tr>
<tr>
<td></td>
<td>Specifies the rule precedence</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-1000&gt; – Specify the value from 1 - 1000.</td>
</tr>
</tbody>
</table>

- deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no deny &lt;STARTING-MAC&gt; &lt;ENDING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>Removes a single device or a set of devices from the deny list</td>
</tr>
<tr>
<td>&lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>To remove a set of devices, enter the MAC address range.</td>
</tr>
<tr>
<td>&lt;ENDING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>Specify the first MAC address in the range.</td>
</tr>
<tr>
<td></td>
<td>Specify the last MAC address in the range.</td>
</tr>
<tr>
<td></td>
<td>Specifies the rule precedence</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-1000&gt; – Specify a value from 1 - 1000.</td>
</tr>
</tbody>
</table>

- no permit <STARTING-MAC> precedence <1-1000>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no permit &lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>Removes a single device or a set of devices from the permit list</td>
</tr>
<tr>
<td>&lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>To remove a single device, enter its MAC address in the &lt;STARTING-MAC&gt; parameter.</td>
</tr>
<tr>
<td></td>
<td>Specifies the rule precedence</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-1000&gt; – Specify a value from 1 - 1000.</td>
</tr>
</tbody>
</table>

- no permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no permit &lt;STARTING-MAC&gt; &lt;ENDING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>Removes a single device or a set of devices from the permit list</td>
</tr>
<tr>
<td>&lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>To remove a set of devices, enter the MAC address range.</td>
</tr>
<tr>
<td>&lt;ENDING-MAC&gt; precedence &lt;1-1000&gt;</td>
<td>Specify the first MAC address in the range.</td>
</tr>
</tbody>
</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
deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160
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)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Adds a device or a set of devices to the deny list</td>
</tr>
<tr>
<td>permit</td>
<td>Adds a device or a set of devices to the permit list</td>
</tr>
</tbody>
</table>
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 — AP300, 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, 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

<table>
<thead>
<tr>
<th>permit &lt;STARTING-MAC&gt; precedence &lt;1-1000&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>permit</strong></td>
</tr>
<tr>
<td><strong>&lt;STARTING-MAC&gt;</strong></td>
</tr>
<tr>
<td><strong>precedence &lt;1-1000&gt;</strong></td>
</tr>
<tr>
<td>• <strong>&lt;1-1000&gt;</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>permit &lt;STARTING-MAC&gt; &lt;ENDING-MAC&gt; precedence &lt;1-1000&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>permit</strong></td>
</tr>
<tr>
<td><strong>&lt;STARTING-MAC&gt;</strong></td>
</tr>
<tr>
<td><strong>&lt;ENDING-MAC&gt;</strong></td>
</tr>
<tr>
<td><strong>precedence &lt;1-1000&gt;</strong></td>
</tr>
<tr>
<td>• <strong>&lt;1-1000&gt;</strong></td>
</tr>
</tbody>
</table>

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><strong>no</strong></td>
<td>Removes a permit rule based on its precedence</td>
</tr>
</tbody>
</table>
CHAPTER 11
ACCESS-LIST

This chapter summarizes IP 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 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 are used as firewalls to filter packets, and may also mark packets, based on the IP address from 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.

MAC ACLs are firewalls that filter or mark packets based on the MAC address from 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.

The following ACLs are supported:

- `ip-access-list`
- `mac-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>
```

**NOTE:** If creating a 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
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)#

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
  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
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)#
11.1 ip-access-list

Table 11.1 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 11-4</td>
</tr>
<tr>
<td>disable</td>
<td>Disables an existing deny or permit rule without removing it from the ACL.</td>
<td>page 11-14</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 11-17</td>
</tr>
<tr>
<td>no</td>
<td>Removes a deny and/or a permit access rule from a IP ACL</td>
<td>page 11-19</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 11-21</td>
</tr>
</tbody>
</table>
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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

`deny [NETWORK-SERVICE-ALIAS-NAME] [icmp|ip|proto|tcp|udp]`

`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>}`

`deny icmp [SOURCE-IP/MASK] [NETWORK-GROUP-ALIAS-NAME] [any] [from-vlan VLAN-ID] [host <SOURCE-HOST-IP>] [DEST-IP/MASK] [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] [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] [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] [any] [host <DEST-HOST-IP>] [log,rule-precedence <1-5000> {rule-description <LINE>}]`

`eq [TCP|UDP] [SOURCE-PORT] [SERVICE-NAME] [bgp|dns|ftp|ftp-data|gopher|https|ldap|ntp|ntp|pop3|sip|smtp|ssh|telnet|ftp|www] [any] [from-vlan VLAN-ID] [host <SOURCE-HOST-IP>] [DEST-IP/MASK] [any] [host <DEST-HOST-IP>] [log,rule-precedence <1-5000> {rule-description <LINE>}]`

**Parameters**

- `deny <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`.
<table>
<thead>
<tr>
<th><strong>&lt;SOURCE-IP/MASK&gt;</strong></th>
<th>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.</th>
</tr>
</thead>
</table>
| **<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). |
| **log** | 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. |
### Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deny</code></td>
<td>Denies packets that match the specified criteria.</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Applies this deny rule to Internet Control Message Protocol (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 dropped.</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 dropped.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the source as any IP address. ICMP packets received from any source are dropped.</td>
</tr>
<tr>
<td><code>from-vlan</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 dropped.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are dropped.</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 dropped.</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 dropped.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the destination as any IP address. ICMP packets addressed to any destination are dropped.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are dropped.</td>
</tr>
</tbody>
</table>

### Examples

- `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> | (rule-description <LINE>) | rule-precedence <1-5000> | log | {<LINE>}`

### Additional Information

- **Marking Packets**
  - Use `mark` to mark packets.
  - `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**
  - `rule-precedence <1-5000>` assigns a precedence for this deny rule.
  - Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
  - `rule-description <LINE>` is optional and describes the purpose of this rule.

### Notes

- Use `from-vlan` with WLANs and port ACLs.

- `any` and `host` are used with the `dscp` and `8021p` parameters.

- `any` and `host` can be used with `source` and `destination` parameters.

- `log` option is supported for logging purposes.

- `rule-description` should not exceed 128 characters in length.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.” 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.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>rule-precedence</code> <code>&lt;1-5000&gt;</code></td>
<td>The following keywords are recursive and common to all of the above parameters: &lt;ul&gt;&lt;li&gt;rule-precedence – Assigns a precedence for this deny rule&lt;/li&gt;&lt;li&gt;<code>&lt;1-5000&gt;</code> – Specify a value from 1 - 5000.&lt;/li&gt;&lt;li&gt;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).&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Applies this deny rule to IP 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. IP packets received from the specified networks are dropped.</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. IP packets received from the addresses identified by the network-group alias are dropped. &lt;ul&gt;&lt;li&gt;<code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code> – Specify the network-group alias name (should be existing and configured). &lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the source as any IP address. IP packets received from any source are dropped.</td>
</tr>
<tr>
<td><code>from-vlan</code> <code>&lt;VLAN-ID&gt;</code></td>
<td>Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are dropped. &lt;ul&gt;&lt;li&gt;<code>&lt;VLAN-ID&gt;</code> – 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. &lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td><code>host</code> <code>&lt;SOURCE-HOST-IP&gt;</code></td>
<td>Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are dropped. &lt;ul&gt;&lt;li&gt;<code>&lt;SOURCE-HOST-IP&gt;</code> – Specify the source host’s exact IP address in the A.B.C.D format. &lt;/li&gt;&lt;/ul&gt;</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. IP packets addressed to the specified networks are dropped.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the destination as any IP address. IP packets addressed to any destination are dropped.</td>
</tr>
<tr>
<td><code>host</code> <code>&lt;DEST-HOST-IP&gt;</code></td>
<td>Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are dropped. &lt;ul&gt;&lt;li&gt;<code>&lt;DEST-HOST-IP&gt;</code> – Specify the destination host’s exact IP address in the A.B.C.D format. &lt;/li&gt;&lt;/ul&gt;</td>
</tr>
</tbody>
</table>
### **deny**

- **proto**
  - Configures the ACL for additional protocols
  - Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter

  | <PROTOCOL-NUMBER> | Filters protocols using their Internet Assigned Numbers Authority (IANA) protocol number
  | <PROTOCOL-NAME> | Filters protocols using their IANA 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.

---

| <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> | 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 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>`
  - `{(rule-description <LINE>)}`
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.

<SOURCE-IP/MASK>
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.

<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).

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 (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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <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.  
**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). |
| tcp | Applies this deny rule to TCP packets only |
| udp | Applies this deny rule to UDP packets only |
| <SOURCE-IP/MASK> | 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. |
| <NETWORK-GROUP-ALIAS-NAME> | 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.  
- **<NETWORK-GROUP-ALIAS-NAME>** – Specify the network-group alias name (should be existing and configured).  
After specifying the source and destination IP address(es), specify the action taken in case of a match. |
| any | 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. |
| from-vlan <VLAN-ID> | This keyword is common to any and ‘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.  
- **<VLAN-ID>** – Specify a 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. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| host <SOURCE-HOST-IP> | Identifies a specific host (as the source to match) by its IP address. TCP/UDP 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>        | 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. |
| any                   | This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are dropped. |
| eq <SOURCE-PORT>     | Identifies a specific source port  
  - <SOURCE-PORT> – Specify the exact source port. |
| host <DEST-HOST-IP>   | Identifies a specific host (as the destination to match) by its IP address. TCP/UDP 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> | 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.  
  - <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). |
| range <START-PORT> <END-PORT> | Specifies a range of source ports  
  - <START-PORT> – Specify the first port in the range.  
  - <END-PORT> – Specify the last port in the range. |
| eq 1-65535 | Identifies a specific destination or protocol port to match  
  - 1-65535 – The destination port is designated by its number  
  - <SERVICE-NAME> – 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)  
    - groper – The designated GROPER protocol port (70)  
    - https – The designated HTTPS protocol port (443)  
    - 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)  
    - POP³ – The designated POP3 protocol port (110)  
    - PPTP – The designated Point-to-Point Tunneling Protocol (PPTP) protocol port (1723)  
    - sip – The designated Session Initiation Protocol (SIP) protocol port (5060)  
    - smtp – The designated Simple Mail Transfer Protocol (SMTP) protocol port (25)  
    - telnet – The designated Telnet protocol port (23)  
    - tftp – The designated Trivial File Transfer Protocol (TFTP) protocol port (69)  
    - www – The designated World Wide Web (WWW) protocol port (80)  
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:

- 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.

**NOTE:** The log option is functional only for router ACLs. The log option displays an informational logging message about the packet that matches the entry sent to the console.
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

rfs7000-37FABE(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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|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

- **disable [deny|permit]**
  - Disables a deny or permit access rule without removing it from the ACL.
  - **Note:** Provide the exact values used to configure the deny or permit rule.

- **<NETWORK-SERVICE-ALIAS-NAME>**
  - Specifies the network-service alias, identified by the `<NETWORK-SERVICE-ALIAS-NAME>` keyword, associated with the deny/permit rule.

- **icmp**
  - Disables a rule applicable to ICMP packets only.

- **ip**
  - Disables a rule applicable to IP packets only.

- **proto <PROTOCOL-OPTIONS>**
  - Disables a rule applicable to any Internet protocol other than TCP, UDP, or ICMP packets.
  - **Note:** After specifying the packet type, specify the source and destination devices and network address(es) to match.

- **tcp**
  - Disables a rule applicable to TCP packets only.

- **udp**
  - Disables a rule applicable to UDP packets only.

- **<SOURCE-IP/MASK>**
  - Specifies the source IP address and mask in the A.B.C.D/M format.

- **<NETWORK-GROUP-ALIAS-NAME>**
  - Specifies the network-group alias, identified by the `<NETWORK-GROUP-ALIAS-NAME>` keyword, associated with this deny/permit rule.

- **any**
  - Select ‘any’ if the rule is applicable to any source IP address.

- **from-vlan <VLAN-ID>**
  - Specify the VLAN IDs.

- **host <SOURCE-HOST-IP>**
  - Specify the source host’s exact IP address.
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
   permit ip host 200.200.200.99 any rule-precedence 3
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
   permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
disable permit ip host 200.200.200.99 any rule-precedence 3
rfs7000-37FABE(config-ip-acl-auto-tunnel-acl)#
```

```
rfs4000-229D58(config-ip-acl-test)#deny icmp any any log rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#
```

```
rfs4000-229D58(config-ip-acl-test)#disable deny icmp any any rule-precedence 1
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>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>permit</strong></td>
<td>Creates a new permit access rule or modifies an existing rule</td>
</tr>
<tr>
<td><strong>alias</strong></td>
<td>Creates and configures a aliases (network, VLAN, and service)</td>
</tr>
</tbody>
</table>
11.1.3 insert

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 an 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
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>` - Provide 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` - After specifying the match rule, specify 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 802.1.p 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>` — 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 new rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).
**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**

<table>
<thead>
<tr>
<th>alias</th>
<th>Creates and configures aliases (network, VLAN, and service)</th>
</tr>
</thead>
</table>
11.1.4 no

- ip-access-list

Removes a deny, permit, or disable rule

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [deny|disable|permit]

no [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]

no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]

Parameters

- no [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp] <RULE-PARAMETERS>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no [deny</td>
<td>permit]</td>
</tr>
<tr>
<td>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</td>
<td>Removes a deny or permit rule applicable to the specified network-service alias</td>
</tr>
<tr>
<td>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify the network-service alias name (should be existing and configured).</td>
<td></td>
</tr>
<tr>
<td>icmp</td>
<td>Removes a deny or permit rule applicable to ICMP packets only</td>
</tr>
<tr>
<td>ip</td>
<td>Removes a deny or permit rule applicable to IP packets only</td>
</tr>
<tr>
<td>proto</td>
<td>Removes a deny or permit rule applicable to protocols (other than IP, ICMP, TCP, and UDP)</td>
</tr>
<tr>
<td>[tcp</td>
<td>udp]</td>
</tr>
<tr>
<td>&lt;RULE-PARAMETERS&gt;</td>
<td>Enter the exact parameters used when configuring the rule.</td>
</tr>
<tr>
<td>rule-precedence</td>
<td>Specify the precedence assigned to this deny/permit rule.</td>
</tr>
<tr>
<td>• rule-description – Optional. Specify the rule description.</td>
<td></td>
</tr>
<tr>
<td>Note: The system removes the rule from the selected ACL.</td>
<td></td>
</tr>
</tbody>
</table>

- no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp] <RULE-PARAMETERS>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no disabled [deny</td>
<td>permit]</td>
</tr>
<tr>
<td>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</td>
<td>Removes a disabled deny or permit rule applicable to the specified network-service alias</td>
</tr>
<tr>
<td>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify the network-service alias name (should be existing and configured).</td>
<td></td>
</tr>
<tr>
<td>icmp</td>
<td>Removes a disabled deny or permit rule applicable to ICMP packets only</td>
</tr>
<tr>
<td>ip</td>
<td>Removes a disabled deny or permit rule applicable to IP packets only</td>
</tr>
</tbody>
</table>
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)#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
```

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Creates a deny access rule</td>
</tr>
<tr>
<td>disable</td>
<td>Disables a deny or permit rule within an IP ACL</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a permit access rule</td>
</tr>
</tbody>
</table>
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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```text
permit [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]


permit icmp [<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>] (<ICMP-TYPE> <ICMP-CODE>,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>|<DEST-IP/MASK>|any|host <DEST-HOST-IP>] (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>})

<table>
<thead>
<tr>
<th><code>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</code></th>
<th>Applies this permit rule to packets based on service protocols and ports specified in the network-service alias</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;NETWORK-SERVICE-ALIAS-NAME&gt;</code> — Specify the network-service alias name (should be existing and configured).</td>
</tr>
</tbody>
</table>

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`. 
<table>
<thead>
<tr>
<th>Clause</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, matching the service protocols and ports specified in the network-service alias, received from the specified network 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. 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.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code> – Specify the network-group alias name (should be existing and configured).</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td><code>any</code></td>
<td>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.</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. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are permitted.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;VLAN-ID&gt;</code> – 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></td>
<td><strong>Note:</strong> Use this option with WLANs and port ACLs.</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. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are permitted.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;SOURCE-HOST-IP&gt;</code> – 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. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are permitted.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed from 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. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified destination are permitted.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEST-HOST-IP&gt;</code> – Specify the destination host’s exact IP address in the A.B.C.D format.</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. Packets, matching the service protocols and ports specified in the network-service alias, addressed for the addresses identified by the network-group alias are permitted.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</code> – Specify the network-group alias name (should be existing and configured).</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. 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>

**Note:**
- Use the `from-vlan` option with WLANs and port ACLs.
- When using a network-group alias, ensure it is existing and configured.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mark</td>
<td>Specifies packets to mark</td>
</tr>
<tr>
<td>{8021p &lt;0-7&gt;}</td>
<td>8021p &lt;0-7&gt; – Marks packets by modifying 802.1p VLAN user priority</td>
</tr>
<tr>
<td>dscp &lt;0-63&gt;</td>
<td>dscp &lt;0-63&gt; – Marks packets by modifying DSCP TOS bits in the header</td>
</tr>
<tr>
<td>rule-precedence</td>
<td>The following keywords are recursive and common to all of the above parameters:</td>
</tr>
<tr>
<td>&lt;1-5000&gt;</td>
<td>rule-precedence – Assigns a precedence for this permit rule</td>
</tr>
<tr>
<td>rule-description</td>
<td>&lt;1-5000&gt; – 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).</td>
</tr>
<tr>
<td>icmp</td>
<td>Applies this permit rule to ICMP packets only</td>
</tr>
<tr>
<td>&lt;SOURCE-IP/MASK&gt;</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>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</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. Note: Use this option with WLANs and port ACLs.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the source as any source IP address. ICMP packets received from any source are permitted.</td>
</tr>
<tr>
<td>from-vlan &lt;VLAN-ID&gt;</td>
<td>Specifies a single VLAN or a range of VL ANs as the match criteria. ICMP packets received from the VL ANs identified here are permitted. Note: Use this option with WLANs and port ACLs.</td>
</tr>
<tr>
<td>host</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>&lt;SOURCE-HOST-IP&gt;</td>
<td>&lt;SOURCE-HOST-IP&gt; – Specify the source host’s exact IP address in the A.B.C.D format.</td>
</tr>
<tr>
<td>&lt;DEST-IP/MASK&gt;</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>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</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. Note: Use this option with WLANs and port ACLs.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies the destination as any destination IP address. ICMP packets addressed to any destination are permitted.</td>
</tr>
<tr>
<td>host</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>&lt;DEST-HOST-IP&gt;</td>
<td>&lt;DEST-HOST-IP&gt; – Specify the destination host’s exact IP address in the A.B.C.D format.</td>
</tr>
</tbody>
</table>
| **<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 permit events matching this entry. If a source and/or destination IP address is matched (i.e. an ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged. |
| **<ICMP-TYPE>** | 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). |

```plaintext
permit 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>)
```

| **ip** | Applies this permit rule to IP packets only |
| **<SOURCE-IP/MASK>** | Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are permitted. |
| **<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.  
• <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 <VLAN-ID>** | Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are permitted.  
• <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 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. 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 <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.
- <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 permitted.
- <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.

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 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).

• 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>) {(rule-description <LINE>)}

proto Configures the ACL for additional protocols
Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter

<PROTOCOL-NUMBER> Filters protocols using their 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.

igmp Identifies the 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.
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igp</td>
<td>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).</td>
</tr>
<tr>
<td>ospf</td>
<td>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.</td>
</tr>
<tr>
<td>vrrp</td>
<td>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.</td>
</tr>
</tbody>
</table>

**<SOURCE-IP/MASK>** 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.

**<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 <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 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 <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 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 <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 permitted.  
  - **<SOURCE-HOST-IP>** – Specify the destination host’s exact IP address in the A.B.C.D format.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <NETWORK-GROUP-ALIAS-NAME>    | Applies a network-group alias to identify the destination IP addresses. Packs (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. |
| 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). |
| tcp                           | Applies this permit rule to TCP packets only                                |
| udp                           | Applies this deny rule to UDP packets only                                 |
| <SOURCE-IP/MASK>              | 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 permitted. |
| <NETWORK-GROUP-ALIAS-NAME>    | 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 permitted.  
  - <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).  
  After specifying the source and destination IP address(es), specify the action taken in case of a match. |
| any                           | This keyword is common to the ‘tcp’ and ‘udp’ parameters.  
  Specifies the source as any source IP address. TCP/UDP packets received from any source are permitted. |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>from-vlan &lt;VLAN-ID&gt;</td>
<td>Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are permitted.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;VLAN-ID&gt;</code> – 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></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>• <code>&lt;SOURCE-HOST-IP&gt;</code> – Specify the source host’s exact IP address in the 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. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP 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. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are permitted.</td>
</tr>
<tr>
<td>eq &lt;SOURCE-PORT&gt;</td>
<td>Identifies a specific source port</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;SOURCE-PORT&gt;</code> – 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.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;DEST-HOST-IP&gt;</code> – 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. 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.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;NETWORK-ALIAS-GROUP-NAME&gt;</code> – 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</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;START-PORT&gt;</code> – Specify the first port in the range.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;END-PORT&gt;</code> – Specify the last port in the range.</td>
</tr>
<tr>
<td>eq</td>
<td>Identifies a specific destination or protocol port to match</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>[&lt;1-65535&gt;]</td>
<td>- The destination port is designated by its number</td>
</tr>
<tr>
<td>&lt;SERVICE-NAME&gt;</td>
<td>- Specifies the service name</td>
</tr>
<tr>
<td>bgp</td>
<td>- The designated <em>Border Gateway Protocol</em> (BGP) protocol port (179)</td>
</tr>
<tr>
<td>dns</td>
<td>- The designated <em>Domain Name System</em> (DNS) protocol port (53)</td>
</tr>
<tr>
<td>ftp</td>
<td>- The designated <em>File Transfer Protocol</em> (FTP) protocol port (21)</td>
</tr>
<tr>
<td>ftp-data</td>
<td>- The designated FTP data port (20)</td>
</tr>
<tr>
<td>gopher</td>
<td>- The designated GROPHER protocol port (70)</td>
</tr>
<tr>
<td>https</td>
<td>- The designated HTTPS protocol port (443)</td>
</tr>
<tr>
<td>ldap</td>
<td>- The designated <em>Lightweight Directory Access Protocol</em> (LDAP) protocol port (389)</td>
</tr>
<tr>
<td>nntp</td>
<td>- The designated <em>Network News Transfer Protocol</em> (NNTP) protocol port (119)</td>
</tr>
<tr>
<td>ntp</td>
<td>- The designated <em>Network Time Protocol</em> (NTP) protocol port (123)</td>
</tr>
<tr>
<td>pop3</td>
<td>- The designated POP3 protocol port (110)</td>
</tr>
<tr>
<td>sip</td>
<td>- The designated <em>Session Initiation Protocol</em> (SIP) protocol port (5060)</td>
</tr>
<tr>
<td>smtp</td>
<td>- The designated <em>Simple Mail Transfer Protocol</em> (SMTP) protocol port (25)</td>
</tr>
<tr>
<td>ssh</td>
<td>- The designated <em>Secure Shell</em> (SSH) protocol port (22)</td>
</tr>
<tr>
<td>telnet</td>
<td>- The designated Telnet protocol port (23)</td>
</tr>
<tr>
<td>tftp</td>
<td>- The designated <em>Trivial File Transfer Protocol</em> (TFTP) protocol port (69)</td>
</tr>
<tr>
<td>www</td>
<td>- The designated www protocol port (80)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>range &lt;START-PORT&gt; &lt;END-PORT&gt;</th>
<th>Specifies a range of destination ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;START-PORT&gt;</td>
<td>- Specify the first port in the range.</td>
</tr>
<tr>
<td>&lt;END-PORT&gt;</td>
<td>- Specify the last port in the range.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>log</th>
<th>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.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>rule-precedence &lt;1-5000&gt;</th>
<th>The following keywords are recursive and common to all of the above:</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**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
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 ACLs. 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

Table 11.2 summarizes MAC 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 a new deny access rule or modifies an existing rule. A deny access rule marks packets for rejection.</td>
<td>page 11-32</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables a MAC deny or permit rule without removing it from the ACL</td>
<td>page 11-35</td>
</tr>
<tr>
<td><code>insert</code></td>
<td>Inserts a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence</td>
<td>page 11-37</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Removes a deny and/or a permit access rule from a MAC ACL</td>
<td>page 11-39</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Creates a new permit access rule or modifies an existing rule. A deny access rule marks packets for forwarding.</td>
<td>page 11-41</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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>]
(dot1p <0-7>,type [8021q|8-165535]|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>]
[<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>]
(dot1p <0-7>,type [8021q|8-165535]|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],
vlan <1-4095>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}

<table>
<thead>
<tr>
<th>`&lt;SOURCE-MAC&gt; &lt;SOURCE-MAC-MASK&gt;</th>
<th>Configures the source MAC address and mask to match</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SOURCE-MAC&gt; — Specify the source MAC address to match.</td>
<td></td>
</tr>
<tr>
<td>&lt;SOURCE-MAC-MASK&gt; — Specify the source MAC address mask.</td>
<td></td>
</tr>
<tr>
<td>Packets received from the specified MAC addresses are dropped.</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Identifies all devices as the source to deny access. Packets received from any source are dropped.</td>
</tr>
<tr>
<td>host &lt;SOURCE-HOST-MAC&gt;</td>
<td>Identifies a specific host as the source to deny access</td>
</tr>
<tr>
<td>&lt;SOURCE-HOST-MAC&gt; — Specify the source host’s exact MAC address to match. Packets received from the specified host are dropped.</td>
<td></td>
</tr>
<tr>
<td>`&lt;DEST-MAC&gt; &lt;DEST-MAC-MASK&gt;</td>
<td>Configures the destination MAC address and mask to match</td>
</tr>
<tr>
<td>&lt;DEST-MAC&gt; — Specify the destination MAC address to match.</td>
<td></td>
</tr>
<tr>
<td>&lt;DEST-MAC-MASK&gt; — Specify the destination MAC address mask to match.</td>
<td></td>
</tr>
<tr>
<td>Packets addressed to the specified MAC addresses are dropped.</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Identifies all devices as the destination to deny access. Packets addressed to any destination are dropped.</td>
</tr>
<tr>
<td>host &lt;DEST-HOST-MAC&gt;</td>
<td>Identifies a specific host as the destination to deny access</td>
</tr>
<tr>
<td>&lt;DEST-HOST-MAC&gt; — Specify the destination host’s exact MAC address to match. Packets addressed to the specified host are dropped.</td>
<td></td>
</tr>
</tbody>
</table>
### 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 takes 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**

```plaintext
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)#
```

```plaintext
rfs4000-229D58(config-mac-acl-test)#deny host 00-01-ae-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

```plaintext
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 MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```plaintext
rfs7000-37FABE(config-mac-acl-test)#deny any host 00:01:ae:00:22:11
rfs7000-37FABE(config-mac-acl-test)#
```

The following example denies traffic between two hosts based on MAC addresses:

```plaintext
rfs7000-37FABE(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host 01:02:89:78:78:45
rfs7000-37FABE(config-mac-acl-test)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes a specified MAC deny access rule</td>
</tr>
</tbody>
</table>
11.2.2 disable

mac-access-list

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

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>, type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp], vlan <1-4095>) log (rule-recedence <1-5000>) {/(rule-description <LINE>)}

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>, type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp], vlan <1-4095>) log (rule-recedence <1-5000>) {/(rule-description <LINE>)

| disable [deny|permit] | Disables a deny 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
| 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
| 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
| dot1p <0-7> | Specify the 802.1p priority from 0 - 7.

Note: Provide the exact values used to configure the deny or permit rule that is to be disabled.
The following example shows the MAC access list ‘test’ settings before the ‘disable’ command is executed:

```
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:

```
rfs4000-229D58(config-mac-acl-test)#disable 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
  disable deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Enables a disabled deny or permit rule</td>
</tr>
<tr>
<td>deny</td>
<td>Creates a new deny access rule or modifies an existing rule</td>
</tr>
<tr>
<td>permit</td>
<td>Creates a new permit access rule or modifies an existing rule</td>
</tr>
</tbody>
</table>
11.2.3 insert

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
insert [deny|permit] <PARAMETERS> (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

- insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>], rule-precedence <1-5000>) {(rule-description <LINE>)}

<p>| insert [deny|permit] | Inserts a deny or permit rule within an MAC ACL |
|----------------------|-----------------------------------------------|
| &lt;PARAMETERS&gt;         | Provide 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. |
| dot1p &lt;0-7&gt;          | Configures the 802.1p priority value. Sets the service classes for traffic handling |
|                      | • &lt;0-7&gt; — Specify 802.1p priority from 0 - 7. |</p>
<table>
<thead>
<tr>
<th>type</th>
<th>Configures the EtherType value</th>
</tr>
</thead>
<tbody>
<tr>
<td>[8021q]&lt;1-65535&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>aarp</td>
<td>appletalk</td>
</tr>
<tr>
<td></td>
<td>- &lt;1-65535&gt; – Indicates the EtherType protocol number</td>
</tr>
<tr>
<td></td>
<td>- aarp – Indicates the Appletalk ARP payload (0x80F3)</td>
</tr>
<tr>
<td></td>
<td>- appletalk – Indicates the Appletalk Protocol payload (0x809B)</td>
</tr>
<tr>
<td></td>
<td>- arp – Indicates the ARP payload (0x0806)</td>
</tr>
<tr>
<td></td>
<td>- ip – Indicates the IPv4 payload (0x0800)</td>
</tr>
<tr>
<td></td>
<td>- ipv6 – Indicates the IPv6 payload (0x86DD)</td>
</tr>
<tr>
<td></td>
<td>- ipx – Indicates the Novell's IPX payload (0x8137)</td>
</tr>
<tr>
<td></td>
<td>- mint – Indicates the MiNT protocol payload (0x8783)</td>
</tr>
<tr>
<td></td>
<td>- rarp – Indicates the reverse ARP payload (0x8035)</td>
</tr>
<tr>
<td></td>
<td>- wisp – Indicates the WISP payload (0x8783)</td>
</tr>
</tbody>
</table>

| vlan <1-4095> | Configures the VLAN where the traffic is received  |
|              | - <1-4095> – Specify the VLAN ID from 1 - 4095.  |

| log | Logs all deny/permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is received from 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-description <LINE> | - 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).  

**Examples**

```
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.
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)#
```
### 11.2.4 `no`

Negates a command or sets its default

Supported in the following platforms:

- **Access Points** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

```plaintext
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>,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

- `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>,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;SOURCE-MAC&gt;</code></td>
<td>Specify the source MAC address and mask</td>
</tr>
<tr>
<td><code>&lt;SOURCE-MAC-MASK&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>any</code></td>
<td>Select ‘any’ if the rule is applicable to any source MAC address</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Specify the source host’s exact MAC address</td>
</tr>
<tr>
<td><code>&lt;DEST-MAC&gt;</code></td>
<td>Specify the destination MAC address and mask</td>
</tr>
<tr>
<td><code>&lt;DEST-MAC-MASK&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>any</code></td>
<td>Identifies all devices as the destination to deny/permit access</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Specify the destination host’s exact MAC address</td>
</tr>
<tr>
<td><code>dot1p &lt;0-7&gt;</code></td>
<td>Specify the 802.1p priority value from 0 -7</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Specify the EtherType value.</td>
</tr>
<tr>
<td>`[8021q</td>
<td>&lt;1-65535&gt;</td>
</tr>
<tr>
<td><code>vlan &lt;1-4095&gt;</code></td>
<td>Specify the VLAN ID.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Select log, if the rule has been configured to log records in case of a match.</td>
</tr>
<tr>
<td><code>mark</code></td>
<td>This is specific to the MAC ACL permit rule. Marks packets that match the ACL rule</td>
</tr>
<tr>
<td>`[8021p &lt;0-7&gt;</td>
<td>dscp &lt;0-63&gt;]`</td>
</tr>
<tr>
<td>no disable [deny</td>
<td>permit] &lt;RULE-PARAMETERS&gt;</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Removes a disabled deny or permit rule from the selected IP access list</td>
<td></td>
</tr>
</tbody>
</table>

| <RULE-PARAMETERS> |
| Enter the exact parameters used when configuring the rule. |

| rule-precedence <1-5000> rule-description <LINE>} |
| Specify the precedence assigned to this disabled deny/permit rule. |
| rule-description – Optional. Specify the rule description. |

**Note:** The system removes the disabled rule from the selected ACL.

**Examples**

```plaintext
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
```

**Related Commands**

<table>
<thead>
<tr>
<th>deny</th>
<th>Creates a MAC deny ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>Creates a MAC permit ACL</td>
</tr>
</tbody>
</table>
### 11.2.5 `permit`

**mac-access-list**

Creating 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|xmp],vlan <1-4095>) log (rule-precedence <1-5000>) {rule-description <LINE>}
```

**Parameters**

- `permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DESTINATION-MAC> <DESTINATION-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|xmp],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>Configures the source MAC address and mask to match</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;SOURCE-MAC&gt;</code></td>
<td>Specifying the source MAC address to match.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;SOURCE-MAC-MASK&gt;</code></td>
<td>Specifying the source MAC address mask.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>&lt;DEST-MAC&gt;</code></th>
<th><code>&lt;DEST-MAC-MASK&gt;</code></th>
<th>Configures the destination MAC address and mask to match</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DEST-MAC&gt;</code></td>
<td>Specifying the destination MAC address to match.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;DEST-MAC-MASK&gt;</code></td>
<td>Specifying the destination MAC address mask to match.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>&lt;SOURCE-MAC&gt;</code></th>
<th><code>&lt;SOURCE-MAC-MASK&gt;</code></th>
<th>Specifies the destination MAC address mask to match</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;SOURCE-MAC&gt;</code></td>
<td>Identifying all devices as the destination to permit access. Packets addressed to any destination are forwarded.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;SOURCE-MAC-MASK&gt;</code></td>
<td>Identifying a specific host as the destination to permit access.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>&lt;DEST-MAC&gt;</code></th>
<th><code>&lt;DEST-MAC-MASK&gt;</code></th>
<th>Specifies the destination MAC address mask to match</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DEST-MAC&gt;</code></td>
<td>Identifying all devices as the destination to permit access. Packets addressed to any destination are forwarded.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;DEST-MAC-MASK&gt;</code></td>
<td>Identifying a specific host as the destination to permit access.</td>
<td></td>
</tr>
</tbody>
</table>

**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.
### 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `dot1p <0-7>` | Configures the 802.1p priority value. Sets the service classes for traffic handling.  
- `<0-7>` – Specify 802.1p priority from 0 - 7. |
| `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). |

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)
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>
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 server policy parameters. To navigate to the config DHCP server policy instance, use the following commands:

```
<DEVICE>(config)#dhcp-server-policy <POLICY-NAME>
```

```
  rfs7000-37FABE(config)#dhcp-server-policy test
  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)#
### 12.1 dhcp-server-policy

Table 12.1 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 12-57</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 12-59</td>
</tr>
<tr>
<td>option</td>
<td>Defines the DHCP option used in DHCP pools</td>
<td>page 12-61</td>
</tr>
<tr>
<td>ping</td>
<td>Specifies ping parameters used by a DHCP server</td>
<td>page 12-62</td>
</tr>
</tbody>
</table>
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 — AP300, 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, 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 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.

Table 12.2 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>
</tbody>
</table>
12.1.2.1 dhcp-class

create 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 — AP300, 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, 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. Table 12.3 summarizes DHCP user class configuration commands.

Table 12.3 DHCP-Class-Config-Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiple-user-class</td>
<td>Enables or disables 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

Enables or disables 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
multiple-user-class
```  

**Parameters**

None

**Examples**

```
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><code>no</code></td>
<td>Disables the multiple user class option for the selected DHCP user class policy</td>
</tr>
</tbody>
</table>
12.1.2.2.2 no

**dhcp-class-mode commands**

Removes this DHCP user class policy’s settings

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [multiple-user-class|option]
no option user-class <VALUE>
```

**Parameters**

- no multiple-user-class
- no option user-class <VALUE>

<table>
<thead>
<tr>
<th>no multiple-user-class</th>
<th>Disables multiple user class options on this DHCP user class policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>no option user-class &lt;VALUE&gt;</td>
<td>Removes the DHCP user class option identified by the &lt;VALUE&gt; keyword</td>
</tr>
</tbody>
</table>

**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
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)#
```

**Related Commands**

- **multiple-user-class** Enables or disables multiple user class option for this DHCP user class policy
- **option** Configures DHCP user class options for this DHCP user class policy
12.1.2.2.3 option

This section describes the configuration of DHCP user class options for this DHCP user class policy.

Supported platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
option user-class <VALUE>
```

Parameters

- **user-class <VALUE>**
  - Configures DHCP user class options
  - `<VALUE>` — Specify the DHCP user class option's ASCII 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. Table 12.4 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 commands</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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

dhcp-pool <POOL-NAME>

Parameters
- dhcp-pool <POOL-NAME>

<POOL-NAME> Creates a DHCP server address pool
- <POOL-NAME> — Specify a name that appropriately identifies this DHCP address pool. If the pool does not exist, it is created. The pool name cannot be modified as part of the edit process. However, an obsolete address pool can be deleted.

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
- dns 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

| no                  | Removes a specified DHCP address pool |
12.1.3.2 dhcp-pool-mode commands

Configures the DHCP pool parameters

Table 12.5 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 12-22</td>
</tr>
<tr>
<td>excluded-address</td>
<td>Prevents a DHCP server from assigning certain addresses to the DHCP pool</td>
<td>page 12-23</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 12-25</td>
</tr>
<tr>
<td>netbios-name-server</td>
<td>Configures a NetBIOS (WINS) name server’s IP address</td>
<td>page 12-26</td>
</tr>
<tr>
<td>netbios-node-type</td>
<td>Defines the NetBIOS node type</td>
<td>page 12-27</td>
</tr>
<tr>
<td>network</td>
<td>Configures the network on which the DHCP server is deployed</td>
<td>page 12-28</td>
</tr>
<tr>
<td>next-server</td>
<td>Configures the next server in the boot process</td>
<td>page 12-29</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 12-36</td>
</tr>
<tr>
<td>static-route</td>
<td>Configures a static route for a DHCP pool</td>
<td>page 12-35</td>
</tr>
<tr>
<td>update</td>
<td>Controls the usage of the DDNS service</td>
<td>page 12-37</td>
</tr>
<tr>
<td>static-binding</td>
<td>Configures static address bindings</td>
<td>page 12-38</td>
</tr>
</tbody>
</table>
### 12.1.3.2.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
address [<IP>|<HOST-ALIAS-NAME>|range]
address [<IP>|<HOST-ALIAS-NAME>|range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]] {class <DHCP-CLASS-NAME>}
```

**Parameters**

- `<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

  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.

- `<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**

```
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>
### 12.1.3.2.2 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
bootfile <IMAGE-FILE-PATH>
```

**Parameters**
- `bootfile <IMAGE-FILE-PATH>`

<table>
<thead>
<tr>
<th>&lt;IMAGE-FILE-PATH&gt;</th>
<th>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.</th>
</tr>
</thead>
</table>

**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**

- `no` | Resets the boot image path for BOOTP clients
- `bootp` | Configures BOOTP protocol parameters
12.1.3.2.3 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 — AP300, 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, 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

- ddns domainname <DDNS-DOMAIN-NAME>
  - domainname
    <DDNS-DOMAIN-NAME>
    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.

- ddns multiple-user-class
  - multiple-user-class
    Enables the multiple user class options with this DDNS domain

- ddns server [<IP>|<HOST-ALIAS-NAME>]
  {<IP1>|<HOST-ALIAS-NAME1>}
  - server
    Configures the DDNS server used by this DHCP profile
    - [<IP>|<HOST-ALIAS-NAME>]
      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.
{<IP1>|<HOST-ALIAS-NAME1>}

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:
- <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.

```
• ddns ttl <1-864000>
```

```
ttl <1-864000>
```

Configures the Time To Live (TTL) value for DDNS updates
- <1-86400> – Specify a value from 1-864000 seconds.

Related Commands

```
no
```

Resets or disables a DHCP pool’s DDNS settings
12.1.3.2.4 default-router

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 — AP300, 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, 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
12.1.3.2.5 dns-server

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 — AP300, 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, 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:
|----------------------|---------------------------------------------------------------
| {IP1|HOST-ALIAS-NAME1} | Optional. Configures the secondary DNS server, using one of the following options:

Note: A maximum of 8 DNS server’s

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
bootstrap 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 DNS server settings
12.1.3.2.6 domain-name

**dhcp-pool-mode commands**

Sets the domain name for the DHCP pool

 Provides 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, computername.domain.com.

Supported in the following platforms:

- Access Points — AP300, 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, 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
ddns server 192.168.13.9
ddns domainname WID
ddns 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
12.1.3.2.7 excluded-address

- dhcp-pool-mode commands

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 — AP300, 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, 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>

  <IP> Adds a single IP address to the excluded address list

- excluded-address <HOST-ALIAS-NAME>

  <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>]

  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>
12.1.3.2.8 lease

dhcp-pool-mode commands

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

lease [0-365]|infinite]
lease infinite
lease <0-365> {<0-23>} {<0-59>} {<0-59>}

Parameters

- lease infinite
  
  infinite | The lease never expires (equal to a static IP address assignment)

- lease <0-365> {<0-23>} {<0-59>} {<0-59>}
  
  <0-365> | Configures the lease duration in days
  
  Note: Days may be 0 only when hours and/or minutes are greater than 0.

- <0-23> | Optional. Sets the lease duration in hours

- <0-59> | Optional. Sets the lease duration in minutes

- <0-59> | Optional. Sets the lease duration in seconds

Usage Guidelines

If lease parameter is not configured on the DHCP pool, the default is used. The default is 24 hours.

Examples

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
  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
  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
12.1.3.2.9 netbios-name-server

**dhcppool-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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>]
{<IP1>|<HOST-ALIAS-NAME1>}
```

**Parameters**

- `netbios-name-server [<IP>|<HOST-ALIAS-NAME>]` (required)
  - 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
  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 192.168.13.25 192.168.13.28
  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
```
12.1.3.2.10 netbios-node-type

Defines the predefined NetBIOS node type. The NetBIOS node type resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — AP300, 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, 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 | h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. |
| m-node | m-node – Sets the node type as mixed. A mixed node uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address. |
| p-node | 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
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
  ddns 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
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

Related Commands

no | Removes the NetBIOS node type settings
12.1.3.2.11 network

- **dhcp-pool-mode commands**

Configures the DHCP server’s network settings

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

    network [<IP/M>|<NETWORK-ALIAS-NAME>]

**Parameters**

- network [<IP/M>|<NETWORK-ALIAS-NAME>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/M&gt;</td>
<td>Configures the network number and mask (for example, 192.168.13.0/24)</td>
</tr>
<tr>
<td>&lt;NETWORK-ALIAS-NAME&gt;</td>
<td>Configures a network alias to identify the network number and mask</td>
</tr>
<tr>
<td></td>
<td>- &lt;NETWORK-ALIAS-NAME&gt; – Specify the network alias name. It should be existing and configured.</td>
</tr>
</tbody>
</table>

**Note:** 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.

**Examples**

rfs4000-229D58 (config-dhcp-policy-test-pool-testPool)#network 192.168.13.0/24

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 192.168.13.25 192.168.13.28
    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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the network number and mask configured for this DHCP pool</td>
</tr>
</tbody>
</table>
12.1.3.2.12 next-server

* dhcp-pool-mode commands

Configures the next server in the boot process

Supported in the following platforms:

- Access Points — AP300, 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, 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><code>&lt;IP&gt;</code></td>
<td>Configures the next server’s (the first server in the boot process) IP address</td>
</tr>
<tr>
<td><code>&lt;HOST-ALIAS-NAME&gt;</code></td>
<td>Configures a host alias, mapped to the next server’s IP address</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#next-server 192.168.13.26
```

```
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
    ddns 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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the next server configuration settings</td>
</tr>
</tbody>
</table>
12.1.3.2.13 no

**dhcp-pool-mode commands**

Removes or resets this DHCP user pool’s settings

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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 [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|netbios-node-type|next-server|network|respond-via-unicast]

| no bootfile | Removes a BOOTP bootfile configuration |
| no default-router | Removes the configured default router for the DHCP pool |
| no dns-server | Removes the configured DNS server for the DHCP pool |
| no domain-name | Removes the configured DNS domain name |
| no lease | Resets the lease to its default (24 hours) |
| no netbios-name-server | Removes the configured NetBIOS name server |
| no netbios-node-type | Removes the NetBIOS node type |
| no next-server | Removes the next server utilized in the boot process |
| no network | Removes the DHCP server network information |
| no respond-via-unicast | Sets the DHCP offer and ACK as broadcast instead of unicast |
- no address [<IP>|<HOST-ALIAS-NAME>|all]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no address</td>
<td>Resets configured DHCP pool addresses</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Removes an IP address from the list of addresses</td>
</tr>
<tr>
<td>&lt;HOST-ALIAS-NAME&gt;</td>
<td>Removes the host alias (used to identify a single host) associated with this DHCP pool's address list</td>
</tr>
<tr>
<td>all</td>
<td>Removes configured DHCP IP addresses</td>
</tr>
</tbody>
</table>

- no address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no address</td>
<td>Resets the DHCP pool addresses</td>
</tr>
<tr>
<td>range [&lt;START-IP&gt;</td>
<td>&lt;START-HOST-ALIAS-NAME&gt;] [&lt;END-IP&gt;</td>
</tr>
<tr>
<td></td>
<td>- &lt;START-IP&gt; – Specify the first IP address in the range.</td>
</tr>
<tr>
<td></td>
<td>- &lt;START-HOST-ALIAS-NAME&gt; – Specify the host alias, mapped to the first IP address in the range.</td>
</tr>
<tr>
<td></td>
<td>- &lt;END-IP&gt; – Specify the last IP address in the range.</td>
</tr>
<tr>
<td></td>
<td>- &lt;END-HOST-ALIAS-NAME&gt; – Specify the host alias, mapped to the last IP address in the range.</td>
</tr>
</tbody>
</table>

Note: The specified IP addresses and host aliases are removed from the DHCP pool's address list.

- no ddns [domainname|multiple-user-class|server|ttl]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ddns</td>
<td>Resets DDNS parameters</td>
</tr>
<tr>
<td>domainname</td>
<td>Removes DDNS domain name information</td>
</tr>
<tr>
<td>multiple-user-class</td>
<td>Resets the use of a multiple user class with the DDNS</td>
</tr>
<tr>
<td>server</td>
<td>Removes configured DDNS servers</td>
</tr>
<tr>
<td>ttl</td>
<td>Resets the TTL information for DDNS updates</td>
</tr>
</tbody>
</table>

- no excluded-address [<IP>|<HOST-ALIAS-NAME>]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no excluded-address &lt;IP&gt;</td>
<td>Removes an excluded IP address from the list of addresses that cannot be issued by the DHCP server</td>
</tr>
<tr>
<td></td>
<td>- &lt;IP&gt; – Specify the IP address.</td>
</tr>
<tr>
<td>&lt;HOST-ALIAS-NAME&gt;</td>
<td>Removes the host alias (used to identify a single host) associated with this DHCP pool's excluded-address list</td>
</tr>
</tbody>
</table>

- no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no excluded-address</td>
<td>Removes a range of excluded IP addresses from the list of addresses that cannot be issued by the DHCP server</td>
</tr>
<tr>
<td>range [&lt;START-IP&gt;</td>
<td>&lt;START-HOST-ALIAS-NAME&gt;] [&lt;END-IP&gt;</td>
</tr>
</tbody>
</table>
no option <OPTION-NAME>

Removes a range of IP addresses and host aliases associated with this DHCP pool’s excluded address list.

- <START-IP> – Specify the first IP address in the range.
- <START-HOST-ALIAS-NAME> – Specify the host alias, mapped to the first IP address in the range.
- <END-IP> – Specify the last IP address in the range.
- <END-HOST-ALIAS-NAME> – Specify the host alias, mapped to the last IP address in the range.

Note: The specified IP addresses and host aliases are removed from the DHCP pool’s excluded address list.

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
    ddns 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)#
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no bootfile
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no network
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no default-router
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no next-server
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no domain-name
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no ddns domainname
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no lease

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
dns-server 192.168.13.19
netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

Related Commands

address  Configures the DHCP server's IP address pool
bootfile  Configures the BOOTP boot file path
ddns     Configures DDNS for use with this DHCP pool
default-router  Configures default routers for this DHCP pool
dns-server  Configures default DNS servers for this DHCP pool
domain-name Configures the DDNS domain name for this DHCP pool
excluded-address Configures IP addresses assigned as static addresses
lease     Configures the DHCP lease settings
netbios-name-server Configures the NetBIOS name server
netbios-node-type  Configures the NetBIOS node type
network   Configures the DHCP server's network settings
next-server Configures the next server in the BOOTP boot process
option    Configures the DHCP option
respond-via-unicast Configures how a DHCP request and ACK are sent
static-binding Configure static binding information
static-route  Configures static routes installed on DHCP clients
update    Controls DDNS service usage
12.1.3.2.14 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 — AP300, 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, 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;OPTION-NAME&gt;</code></td>
<td>Sets the name of the DHCP option</td>
</tr>
<tr>
<td><code>&lt;DHCP-OPTION-IP&gt;</code></td>
<td>Sets DHCP option as an IP address</td>
</tr>
<tr>
<td><code>&lt;DHCP-OPTION-ASCII&gt;</code></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
12.1.3.2.15 static-route

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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
12.1.3.2.16 respond-via-unicast

- dhcp-pool-mode commands

Sends DHCP offer and acknowledgement as unicast messages

Supported in the following platforms:
- Access Points — AP300, 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, 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. |
12.1.3.2.17 update

dhcp-pool-mode commands

Controls the use of the DDNS service

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
update dns {override}

Parameters
- update dns {override}

<table>
<thead>
<tr>
<th>dns {override}</th>
<th>Configures DDNS parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>override</td>
<td>Optional. Enables DDNS updates on an onboard DHCP server</td>
</tr>
</tbody>
</table>

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
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

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.

Table 12.6 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 12-39</td>
</tr>
<tr>
<td>static-binding-mode commands</td>
<td>Invokes static binding configuration commands</td>
<td>page 12-41</td>
</tr>
</tbody>
</table>
12.1.3.3.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

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
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)#] static-binding client-identifier test

[rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#]?
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

rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#static-binding hardware-address 11-22-33-44-55-66
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#?

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

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets values or disables the DHCP policy static binding settings</td>
</tr>
<tr>
<td>static-binding-mode commands</td>
<td>Invokes static binding configuration commands</td>
</tr>
</tbody>
</table>
### 12.1.3.3.2 static-binding-mode commands

- **static-binding**

Table 12.7 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 12-42</td>
</tr>
<tr>
<td>client-name</td>
<td>Configures a client name</td>
<td>page 12-43</td>
</tr>
<tr>
<td>default-router</td>
<td>Configures default router or gateway IP address</td>
<td>page 12-44</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 12-45</td>
</tr>
<tr>
<td>domain-name</td>
<td>Sets the network pool’s domain name</td>
<td>page 12-47</td>
</tr>
<tr>
<td>ip-address</td>
<td>Configures a host’s fixed IP address</td>
<td>page 12-48</td>
</tr>
<tr>
<td>netbios-name-server</td>
<td>Configures a NetBIOS (WINS) name server IP address</td>
<td>page 12-49</td>
</tr>
<tr>
<td>netbios-node-type</td>
<td>Defines the NetBIOS node type</td>
<td>page 12-50</td>
</tr>
<tr>
<td>next-server</td>
<td>Specifies the next server used in the boot process</td>
<td>page 12-51</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 12-52</td>
</tr>
<tr>
<td>option</td>
<td>Configures raw DHCP options</td>
<td>page 12-54</td>
</tr>
<tr>
<td>respond-via-unicast</td>
<td>Sends a DHCP offer and DHCP Ack as unicast messages</td>
<td>page 12-55</td>
</tr>
<tr>
<td>static-route</td>
<td>Adds static routes installed on DHCP clients</td>
<td>page 12-56</td>
</tr>
</tbody>
</table>
12.1.3.3 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 — AP300, 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, 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 parameters
12.1.3.4 client-name

*static-binding-mode commands*

Configures the client's name

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
client-name <NAME>
```

**Parameters**

- client-name <NAME>

<table>
<thead>
<tr>
<th>&lt;NAME&gt;</th>
<th>Specify the name of the client using this static IP address host pool. Do not include the domain name.</th>
</tr>
</thead>
</table>

**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
  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
### 12.1.3.3.5 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 — AP300, 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, 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
client-name RFID bootfile test.txt
default-router 172.16.10.8 172.16.10.9
```

**Related Commands**

- `no` Resets values or disables DHCP pool static binding settings
12.1.3.3.6 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 — AP300, 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, 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

| `<HOST-ALIAS-NAME>` `<HOST-ALIAS-NAME1>` | Configures the primary DNS server’s host alias. The host alias is mapped to the DNS server’s IP address, and should be existing and configured.
| --- | --- |
| `<HOST-ALIAS-NAME>` – Optional. Configures the secondary DNS server’s host alias (if configured). 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`.

| `{<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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets values or disables DHCP pool static binding settings</td>
</tr>
</tbody>
</table>
12.1.3.7 domain-name

`static-binding-mode commands`

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

domain-name <DOMAIN-NAME>

**Parameters**

- domain-name <DOMAIN-NAME>

| <DOMAIN-NAME> | Defines the domain name for the static binding configuration |

**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
client-name RFID
domain-name documentation
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
```

**Related Commands**

| `no` | Resets values or disables the DHCP pool static binding settings |
### 12.1.3.3.8 ip-address

*static-binding-mode commands*

Configures a fixed IP address for a host

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
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**

```
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><em>no</em></td>
<td>Resets values or disables DHCP pool static binding settings</td>
</tr>
</tbody>
</table>
### 12.1.3.9 netbios-name-server

- **static-binding-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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

**Parameters**
- `<IP>` or `<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.

**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
  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
  netbios-name-server 172.16.10.23
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

**Related Commands**

- **no**
  - Resets values or disables DHCP pool static binding settings
12.1.3.10 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 — AP300, 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, 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]

<table>
<thead>
<tr>
<th>[b-node]</th>
<th>h-node</th>
<th>m-node</th>
<th>p-node</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>b-node</td>
<td>h-node</td>
<td>m-node</td>
<td>p-node</td>
<td>Defines the netbios node type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- b-node — Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- h-node — Sets the node type as hybrid. Uses a combination of two or more nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- m-node — Sets the node type as mixed. A mixed node uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
</tbody>
</table>

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
   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
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

Related Commands
- no | Resets values or disables DHCP pool static binding settings
**12.1.3.3.11 next-server**

*static-binding-mode commands*

Configures the next server utilized in the boot process.

Supported in the following platforms:
- Access Points — AP300, 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, 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><code>&lt;IP&gt;</code></td>
<td>Configures the next server's (the first server in the boot process) IP address</td>
</tr>
<tr>
<td><code>&lt;HOST-ALIAS-NAME&gt;</code></td>
<td>Configures a host alias, mapped to the next server’s IP address</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;HOST-ALIAS-NAME&gt;</code> — Specify the host alias name. It should be existing and configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A network host alias maps a name to a single network host. For example, ‘alias host $HOST 1.1.1.100’. In this example the host alias is <code>$HOST</code> and it maps to a single host <code>1.1.1.100</code>. For more information, see <em>alias</em>.</td>
</tr>
</tbody>
</table>

**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
12.1.3.3.12 no

Negates or reverts static binding settings for the selected DHCP server policy

Supported in the following platforms:

- Access Points — AP300, 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, 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 [bootfile|client-name|default-router|dns-server|domain-name|ip-address|
  netbios-name-server|netbios-node-type|next-server|option|respond-via-unicast]

| no bootfile | Removes the BOOTP bootfile configuration |
| no client-name | Removes the client name from the static binding configuration |
| no default-router | Removes the default router from the static binding configuration |
| no dns-server | Removes the DNS server from the static binding configuration |
| no domain-name | Removes the DNS domain name |
| no ip-address | Removes IP addresses from the static binding configuration |
| no netbios-name-server | Removes the NetBIOS name server |
| no netbios-node-type | Removes the NetBIOS node type |
| no next-server | Removes the next server utilized in the boot process |
| no respond-via-unicast | Sets the DHCP offer and ACK as broadcast instead of unicast |

- no option <OPTION-NAME>

| no option <OPTION-NAME> | Resets the DHCP option to the value specified by the <OPTION-NAME> parameter |

- no static-route <IP/MASK> <GATEWAY-IP>

| no static-route | Removes static routes from the static binding configuration |
| <IP/MASK> | Removes information for a particular subnet |
| <GATEWAY-IP> | Removes gateway information from a particular subnet's routing information |
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-name-server 172.16.10.23
    next-server 172.16.10.24
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>bootfile</td>
<td>Configures the BOOTP boot file path</td>
</tr>
<tr>
<td>client-name</td>
<td>Configures a host's name</td>
</tr>
<tr>
<td>default-router</td>
<td>Configures default routers for a DHCP pool</td>
</tr>
<tr>
<td>dns-server</td>
<td>Configures default DNS servers for a DHCP pool</td>
</tr>
<tr>
<td>domain-name</td>
<td>Configures the DDNS domain name for a DHCP pool</td>
</tr>
<tr>
<td>ip-address</td>
<td>Configures IP addresses assigned to a host</td>
</tr>
<tr>
<td>netbios-name-server</td>
<td>Configures the NetBIOS name server</td>
</tr>
<tr>
<td>netbios-node-type</td>
<td>Configures the NetBIOS node type</td>
</tr>
<tr>
<td>next-server</td>
<td>Configures the next server utilized in the BOOTP boot process</td>
</tr>
<tr>
<td>option</td>
<td>Configures the DHCP option</td>
</tr>
<tr>
<td>respond-via-unicast</td>
<td>Configures the DHCP request and ACK sending mode (broadcast or unicast)</td>
</tr>
<tr>
<td>static-route</td>
<td>Configures the static binding's route</td>
</tr>
</tbody>
</table>
12.1.3.3.13 option

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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**

```plaintext
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#option option1 172.16.10.10
```

```plaintext
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)#
```
12.1.3.3.14 respond-via-unicast

*static-binding-mode commands*

Sends a DHCP offer and DHCP acknowledge as unicast messages

Supported in the following platforms:
- Access Points — AP300, 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, 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

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

**Related Commands**

| no | Resets values or disables DHCP pool static binding settings |
12.1.3.3.15 static-route

**static-binding-mode commands**

Adds static routes to the static binding configuration

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
static-route <IP/MASK> <GATEWAY-IP>
```

**Parameters**

- `static-route <IP/MASK> <GATEWAY-IP>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP/MASK&gt;</code></td>
<td>Sets the subnet for which the static route is configured</td>
</tr>
<tr>
<td><code>&lt;GATEWAY-IP&gt;</code></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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master <1-255>]

**Parameters**

- dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master <1-255>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-server</td>
<td>Enables/disables dynamic activation of the DHCP server, running on a redundancy device, based on the activation criteria specified</td>
</tr>
<tr>
<td>activation-criteria [cluster-master</td>
<td>rf-domain-manager</td>
</tr>
<tr>
<td>cluster-master</td>
<td>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>rf-domain-manager</td>
<td>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>vrrp-master &lt;1-255&gt;</td>
<td>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
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

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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 bootp ignore
- no dhcp-class <DHCP-CLASS-NAME>
- no dhcp-pool <DHCP-POOL-NAME>
- no dhcp-server activation-criteria
- no option <DHCP-OPTION>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no bootp</td>
<td>Removes the BOOTP specific configuration</td>
</tr>
<tr>
<td>ignore</td>
<td>Removes the DHCP server ignoring BOOTP requests</td>
</tr>
<tr>
<td>no dhcp-class &lt;DHCP-CLASS-NAME&gt;</td>
<td>Removes a specified DHCP class</td>
</tr>
<tr>
<td></td>
<td>• &lt;DHCP-CLASS-NAME&gt; – Specifies the DHCP class name</td>
</tr>
<tr>
<td>no dhcp-pool &lt;DHCP-POOL-NAME&gt;</td>
<td>Removes a specified DHCP pool</td>
</tr>
<tr>
<td></td>
<td>• &lt;DHCP-POOL-NAME&gt; – Specifies the DHCP pool name</td>
</tr>
<tr>
<td>no dhcp-server activation-criteria</td>
<td>Removes the DHCP service activation criteria configured on this DHCP server policy</td>
</tr>
<tr>
<td>no option &lt;DHCP-OPTION&gt;</td>
<td>Removes a DHCP option</td>
</tr>
<tr>
<td>&lt;DHCP-OPTION&gt;</td>
<td>Sets the DHCP option</td>
</tr>
</tbody>
</table>
- **no ping timeout**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ping timeout</td>
<td>Resets the DHCP server ping timeout</td>
</tr>
<tr>
<td>timeout</td>
<td>Resets the timeout to its default</td>
</tr>
</tbody>
</table>

### 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)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootp</td>
<td>Configures the BOOTP protocol parameters</td>
</tr>
<tr>
<td>dhcp-class</td>
<td>Configures the DHCP user class parameters</td>
</tr>
<tr>
<td>dhcp-pool</td>
<td>Configures the DHCP pool</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>
</tr>
<tr>
<td>option</td>
<td>Configures the DHCP options</td>
</tr>
<tr>
<td>ping</td>
<td>Configures the DHCP ping timeout</td>
</tr>
</tbody>
</table>
12.1.6 **option**

* dhcp-server-policy

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
option <OPTION-NAME> <0-250> [ascii|hexstring|ip]
```

**Parameters**

- option <OPTION-NAME> <0-250> [ascii|hexstring|ip]

<table>
<thead>
<tr>
<th>&lt;OPTION-NAME&gt;</th>
<th>Configures the option name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-250&gt;</td>
<td>Configures the DHCP option code from 0 - 250</td>
</tr>
<tr>
<td>ascii</td>
<td>Configures the DHCP option as an ASCII string</td>
</tr>
<tr>
<td>hexstring</td>
<td>Configures the DHCP option as a hexadecimal string</td>
</tr>
<tr>
<td>ip</td>
<td>Configures the DHCP option as an IP address</td>
</tr>
</tbody>
</table>

**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**

```
rfs7000-37FABE(config-dhcp-policy-test)#option option1 200 ascii
rfs7000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
  option option1 200 ascii
rfs7000-37FABE(config-dhcp-policy-test)#
```

**Related Commands**

- `no` Removes DHCP server options
### 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

`ping timeout <1-10>`

**Parameters**
- `ping timeout <1-10>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout &lt;1-10&gt;</code></td>
<td>Sets the ping timeout from 1 - 10 seconds. The default is 1 second.</td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets the ping interval to 1 second</td>
</tr>
</tbody>
</table>
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:

```console
rfs7000-37FABE(config)#firewall-policy <POLICY-NAME>
```

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
- logging: Firewall enhanced logging
- no: Negate a command or set its defaults
- proxy-arp: Enable generation of ARP responses 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)
- 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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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)#
13.1 firewall-policy

Table 13.1 summarizes default firewall policy configuration commands.

Table 13.1 Firewall-Policy-Config 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 tunneled packets</td>
<td>page 13-6</td>
</tr>
<tr>
<td>dhcp-offer-convert</td>
<td>Enables the conversion of broadcast DHCP offers to unicast</td>
<td>page 13-7</td>
</tr>
<tr>
<td>dns-snoop</td>
<td>Sets the timeout value for DNS entries</td>
<td>page 13-8</td>
</tr>
<tr>
<td>firewall</td>
<td>Configures the wireless firewall</td>
<td>page 13-9</td>
</tr>
<tr>
<td>flow</td>
<td>Defines a session flow timeout</td>
<td>page 13-10</td>
</tr>
<tr>
<td>ip</td>
<td>Sets an IP address for a selected device</td>
<td>page 13-12</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>logging</td>
<td>Enables enhanced firewall logging</td>
<td>page 13-23</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 13-25</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>stateful-packet-inspection-12</td>
<td>Enables stateful packets-inspection in layer 2 firewall</td>
<td>page 13-33</td>
</tr>
<tr>
<td>storm-control</td>
<td>Defines storm control and logging settings</td>
<td>page 13-34</td>
</tr>
<tr>
<td>virtual-defragmentation</td>
<td>Enables virtual defragmentation of IPv4 packets</td>
<td>page 13-36</td>
</tr>
</tbody>
</table>
13.1.1 acl-logging

**firewall-policy**

Enables logging on flow creating traffic

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
_acl-logging
```

**Parameters**

None

**Examples**

```
rfs4000-229D58 (config-fw-policy-test)#acl-logging
rfs4000-229D58 (config-fw-policy-test)#
rfs4000-229D58 (config-fw-policy-test)#no acl-logging
rfs4000-229D58 (config-fw-policy-test)#
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><code>no</code></td>
<td>Disables logging on flow creating traffic</td>
</tr>
</tbody>
</table>
13.1.2 alg

*firewall-policy*

Enables preconfigured algorithms supporting a particular protocol

The Firewall policy allows traffic filtering at the application layer using the *Application Layer Gateway (ALG)* feature

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
alg [dns|facetime|ftp|sccp|sip|tftp]
```

**Parameters**

- `alg [dns|facetime|ftp|sccp|sip|tftp]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alg</td>
<td>Enables preconfigured algorithms. The default is enabled.</td>
</tr>
<tr>
<td>dns</td>
<td>Enables the <em>Domain Name System (DNS)</em> algorithm. The default is enabled.</td>
</tr>
<tr>
<td>facetime</td>
<td>Enables the FaceTime algorithm. The default is enabled.</td>
</tr>
<tr>
<td>ftp</td>
<td>Enables the <em>File Transfer Protocol (FTP)</em> algorithm. The default is enabled.</td>
</tr>
<tr>
<td>sccp</td>
<td>Enables the <em>Skinny Call Control Protocol (SCCP)</em> algorithm. The default is enabled.</td>
</tr>
<tr>
<td>sip</td>
<td>Enables the <em>Session Initiation Protocol (SIP)</em> algorithm. The default is enabled.</td>
</tr>
<tr>
<td>tftp</td>
<td>Enables the <em>Trivial File Transfer Protocol (TFTP)</em> algorithm. The default is enabled.</td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-fw-policy-test)#alg tftp
```

**Related Commands**

```
no
```

Disables or resets a specified algorithm
13.1.3 clamp

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.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
clamp tcp-mss

Parameters
- clamp tcp-mss

| tcp-mss | Limits the TCP MSS size to the MTU value of the inner protocol for tunneled packets |

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 — AP300, 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, 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

Supported in the following platforms:
- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

dns-snoop entry-timeout <30-86400>

**Parameters**
- **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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
firewall enable

Parameters
- firewall enable

<table>
<thead>
<tr>
<th>firewall enable</th>
<th>Enables wireless firewalls</th>
</tr>
</thead>
</table>

Examples
rfs7000-37FABE(config-fw-policy-default)#firewall enable
rfs7000-37FABE(config-fw-policy-default)#

Related Commands
- no
  | Disables a device's firewall |
### 13.1.7 flow

- **firewall-policy**

Defines the session flow timeout interval for different packet types

Supported in the following platforms:
- Access Points — AP300, 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, 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**

<table>
<thead>
<tr>
<th>dhcp</th>
<th>Configures DHCP packet flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>stateful</td>
<td>Performs a stateful check on DHCP packets. This feature is enabled by default.</td>
</tr>
</tbody>
</table>

- **flow timeout [icmp|other] <1-32400>**

<table>
<thead>
<tr>
<th>timeout</th>
<th>Configures a packet timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp</td>
<td>Configures the timeout for ICMP packets. The default is 30 seconds.</td>
</tr>
<tr>
<td>other</td>
<td>Configures the timeout for packets other than ICMP, TCP, or UDP. The default is 30 seconds.</td>
</tr>
<tr>
<td>&lt;1-32400&gt;</td>
<td>Configures the timeout from 1 - 32400 seconds</td>
</tr>
</tbody>
</table>

- **flow timeout udp <15-32400>**

<table>
<thead>
<tr>
<th>timeout</th>
<th>Configures a packet timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp</td>
<td>Configures the timeout for UDP packets. The default is 30 seconds.</td>
</tr>
<tr>
<td>15-32400&gt;</td>
<td>Configures the timeout from 15 - 32400 seconds</td>
</tr>
</tbody>
</table>

- **flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|stateless-general] <1-32400>**

<table>
<thead>
<tr>
<th>timeout</th>
<th>Configures a packet timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Configures the timeout for TCP packets</td>
</tr>
<tr>
<td>close-wait</td>
<td>Configures the closed TCP flow timeout. The default is 10 seconds.</td>
</tr>
<tr>
<td>reset</td>
<td>Configures the reset TCP flow timeout. The default is 10 seconds.</td>
</tr>
<tr>
<td>setup</td>
<td>Configures the opening TCP flow timeout. The default is 10 seconds.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stateless Fin-or-Reset</td>
<td>Configures stateless TCP flow timeout created with the FIN or RESET packets. The default is 10 seconds.</td>
</tr>
<tr>
<td>Stateless General</td>
<td>Configures the stateless TCP flow timeout. The default is 90 seconds (1m 30 s).</td>
</tr>
<tr>
<td>1-32400</td>
<td>Configures the timeout from 1 - 32400 seconds</td>
</tr>
</tbody>
</table>

**Examples**

```
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
```

```
rfs7000-37FABE(config-fw-policy-test)#show context firewall-policy test
  no ip dos tcp-sequence-past-window
  flow timeout icmp 16000
  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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes session timeout intervals configured for different packet types</td>
</tr>
</tbody>
</table>
13.1.8 ip

`firewall-policy`

Configures Internet Protocol (IP) components

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ip [dos|tcp]
```

```
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|
tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|
tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|
udp-short-hdr|winnuke}
```

```
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|
tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|
tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke} [log-and-drop|log-only] log-level [0-7] [alerts|critical|debug|emergencies|errors|informational|notifications|warnings]
```

```
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|
tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|
tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke} [drop-only]
```

```
ip dos tcp-max-incomplete [high|low] <1-1000>
```

```
ip tcp [adjust-mss|optimize-unecessary-resends|recreate-flow-on-out-of-state-syn|
validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

```
ip tcp adjust-mss <472-1460>
```

```
ip tcp [optimize-unecessary-resends|recreate-flow-on-out-of-state-syn|
validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

**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>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast-multicast-icmp</td>
<td>Optional. Detects broadcast or multicast ICMP DoS attacks. 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.</td>
</tr>
<tr>
<td>chargen</td>
<td>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.</td>
</tr>
<tr>
<td>fraggle</td>
<td>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.</td>
</tr>
<tr>
<td>ftp-bounce</td>
<td>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.</td>
</tr>
<tr>
<td>invalid-protocol</td>
<td>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.</td>
</tr>
<tr>
<td>ip-ttl-zero</td>
<td>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.</td>
</tr>
<tr>
<td>ipsproof</td>
<td>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.</td>
</tr>
<tr>
<td>land</td>
<td>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.</td>
</tr>
<tr>
<td>option-route</td>
<td>Optional. Enables an IP Option Record Route DoS check.</td>
</tr>
</tbody>
</table>
router-advt
This attack uses ICMP to redirect the network router function to some other host. If that host
can not 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).

router-solicit
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). (For more information about
the process of ICMP router solicitation, see “Routing Sequences for ICMP.”)
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.

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.

tcp-fin-scan
Optional. Detects TCP FIN scan attacks
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.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 large amount of data to UDP port 137 to crash the NETBIOS service on Windows and results in high CPU 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 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 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 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.</td>
</tr>
<tr>
<td>invalid-protocol</td>
<td>Optional. Enables a check for invalid protocol number</td>
</tr>
<tr>
<td>ip-ttl-zero</td>
<td>Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ipsproof</td>
<td>Optional. Enables a check for IP spoofing DoS attack</td>
</tr>
<tr>
<td>land</td>
<td>Optional. 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.</td>
</tr>
<tr>
<td>option-route</td>
<td>Optional. Enables an IP Option Record Route DoS check</td>
</tr>
<tr>
<td>router-advt</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>router-solicit</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>smurf</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>snork</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>tcp-bad-sequence</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>tcp-fin-scan</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>tcp-intercept</td>
<td>Optional. Prevents TCP intercept attacks by using TCP SYN cookies</td>
</tr>
<tr>
<td>tcp-null-scan</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>tcp-post-syn</td>
<td>Optional. Enables a TCP post SYN DoS attack</td>
</tr>
<tr>
<td>tcp-sequence-pastwindow</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>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, causing devices to crash with a blue screen.</td>
</tr>
<tr>
<td>drop-only</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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos</td>
<td>Identifies IP events as DoS events</td>
</tr>
<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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Identifies and configures TCP events and configuration items</td>
</tr>
<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>

### ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Identifies and configures TCP events and configuration items</td>
</tr>
<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)#ip dos fraggle drop-only
rfs7000-37FABE(config-fw-policy-test)#ip dos tcp-sequence-past-window drop-only
rfs7000-37FABE(config-fw-policy-test)#ip dos tcp-max-incomplete high 600
rfs7000-37FABE(config-fw-policy-test)#ip dos tcp-max-incomplete low 60
rfs7000-37FABE(config-fw-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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets firewall policy IP components</td>
</tr>
</tbody>
</table>
13.1.9 ip-mac

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
ip-mac [conflict|routing]
ip-mac conflict drop-only
ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
   emergencies|errors|informational|notifications|warnings]
ip-mac routing conflict drop-only
ip-mac routing [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 an 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>

• **ip-mac routing** `[log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|emergencies|errors|informational|notifications|warnings]`

<table>
<thead>
<tr>
<th>routing</th>
<th>Defines a routing table based action</th>
</tr>
</thead>
<tbody>
<tr>
<td>conflict</td>
<td>Action performed when a conflict exists in the routing table. 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 to log this event under</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 an 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>

**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
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)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables actions based on device IP MAC table, IP address, and MAC address conflict detection</td>
</tr>
</tbody>
</table>
13.1.10 logging

Configures enhanced firewall logging

Supported in the following platforms:

- Access Points — AP300, 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, 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

<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>

- logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]

<table>
<thead>
<tr>
<th>logging</th>
<th>Configures enhanced firewall logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-packet-drop</td>
<td>Drops ICMP packets that do not pass sanity checks. The default is none.</td>
</tr>
<tr>
<td>malformed-packet-drop</td>
<td>Drops raw IP 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

rfs7000-37FABE(config-rw-policy-test)#logging verbose
rfs7000-37FABE(config-rw-policy-test)#logging icmp-packet-drop rate-limited
rfs7000-37FABE(config-rw-policy-test)#logging malformed-packet-drop all
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
  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
rfs7000-37FABE(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>Disables enhanced firewall logging</td>
</tr>
</tbody>
</table>
### 13.1.11 no

**firewall-policy**

Negates a command or sets the default for firewall policy commands.

Supported in the following platforms:
- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [acl-logging|alg|clamp|dhcp-offer-convert|dns-snoop|firewall|flow|ip|ip-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|sip|sccp|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 ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|
invalid-protocol|ip-ttl-zero|ipproof|land|option-route|router-advt|router-solicit|
smf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-syn|
tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke}
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 ip-mac routing conflict
no logging [icmp-packet-drop|verbose|malformed-packet-drop]
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|maximun-defragmentation-per-host}
```

**Parameters**

- **no [acl-logging|dhcp-offer-convert|proxy-arp|stateful-packet-inspection-l2]**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no acl-logging</td>
<td>Disables logging of flow creating traffic</td>
</tr>
<tr>
<td>no dhcp-offer-convert</td>
<td>Disables the conversion of broadcast DHCP offers to unicast</td>
</tr>
<tr>
<td>no proxy-arp</td>
<td>Disables the generation of ARP responses on behalf of other devices</td>
</tr>
</tbody>
</table>
| no stateful-packet-
  inspection-l2           | Disables layer 2 stateful packet inspection                                 |

**Parameters (continued):**

- **no acl-logging**
- **no dhcp-offer-convert**
- **no proxy-arp**
- **no stateful-packet-inspection-l2**

---

**Supported in the following platforms:**

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`no alg [dns</td>
<td>facetime</td>
</tr>
<tr>
<td><code>no alg</code></td>
<td>Disables the DNS algorithm</td>
</tr>
<tr>
<td><code>dns</code></td>
<td>Disables the DNS algorithm</td>
</tr>
<tr>
<td><code>facetime</code></td>
<td>Disables the Facetime algorithm</td>
</tr>
<tr>
<td><code>ftp</code></td>
<td>Disables the FTP algorithm</td>
</tr>
<tr>
<td><code>sccp</code></td>
<td>Disables the SCCP algorithm</td>
</tr>
<tr>
<td><code>sip</code></td>
<td>Disables the SIP algorithm</td>
</tr>
<tr>
<td><code>tftp</code></td>
<td>Disables the TFTP algorithm</td>
</tr>
<tr>
<td><code>no clamp tcp-mss</code></td>
<td>Disables TCP MSS size limiting to the size of the MTU in the inner protocol of a tunneled packet</td>
</tr>
<tr>
<td><code>no dns-snoop entry-timeout</code></td>
<td>Disables DNS snooping</td>
</tr>
<tr>
<td><code>no dns</code></td>
<td>Disables DNS snooping</td>
</tr>
<tr>
<td><code>entry-timeout</code></td>
<td>Disables DNS snoop table entry timeout</td>
</tr>
<tr>
<td><code>no firewall enable</code></td>
<td>Disables a device’s firewalls</td>
</tr>
<tr>
<td><code>no flow dhcp stateful</code></td>
<td>Disables firewall flows</td>
</tr>
<tr>
<td><code>no dhcp stateful</code></td>
<td>Disables DHCP stateful flow</td>
</tr>
<tr>
<td>`no flow timeout [icmp</td>
<td>other</td>
</tr>
<tr>
<td><code>timeout</code></td>
<td>Disables the timeout for various packet types</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Disables ICMP packet timeout</td>
</tr>
<tr>
<td><code>others</code></td>
<td>Disables the timeout for packets other than TCP, ICMP, or UDP</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Disables UDP packet timeout</td>
</tr>
<tr>
<td>`no flow timeout tcp [closed-wait</td>
<td>established</td>
</tr>
<tr>
<td><code>no flow</code></td>
<td>Disables firewall flows</td>
</tr>
<tr>
<td><code>timeout</code></td>
<td>Disables the timeout for various packet types</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Disables TCP packet timeout</td>
</tr>
<tr>
<td><code>close-wait</code></td>
<td>Disables the timeout for TCP flows in close wait status</td>
</tr>
<tr>
<td><code>established</code></td>
<td>Disables the timeout for TCP flows in established status</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reset</td>
<td>Disables the timeout for TCP flows in reset status</td>
</tr>
<tr>
<td>setup</td>
<td>Disables the timeout for TCP flows in setup status</td>
</tr>
<tr>
<td>stateless-fin-or-reset</td>
<td>Disables the timeout for TCP flows in stateless FIN or RST status</td>
</tr>
<tr>
<td>stateless-general</td>
<td>Disables the timeout for TCP flows in general stateless states</td>
</tr>
<tr>
<td>no ip</td>
<td>Disables IP events</td>
</tr>
<tr>
<td>dos</td>
<td>Disables IP DoS events</td>
</tr>
<tr>
<td>ascend</td>
<td>Optional. Disables an ASCEND DoS check</td>
</tr>
<tr>
<td></td>
<td>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>broadcast-multicast-icmp</td>
<td>Optional. Disables the detection of broadcast or multicast ICMP packets as an attack</td>
</tr>
<tr>
<td>chargen</td>
<td>Optional. Disables the chargen service</td>
</tr>
<tr>
<td></td>
<td>The Character Generation Protocol (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a generic payload for bandwidth and QoS measurements.</td>
</tr>
<tr>
<td>fraggle</td>
<td>Optional. Disables checking for Fraggle DoS attacks. This checks for UDP packets to or from port 7 or 19</td>
</tr>
<tr>
<td>ftp-bounce</td>
<td>Optional. Disables FTP bounce attack checks</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>invalid-protocol</td>
<td>Optional. Disables a check for invalid protocol number</td>
</tr>
<tr>
<td>ip-ttl-zero</td>
<td>Optional. Disables a check for the TCP/IP TTL field with a value of Zero (0)</td>
</tr>
<tr>
<td>ipsproof</td>
<td>Optional. Disables IP spoofing DoS attack checks</td>
</tr>
<tr>
<td>land</td>
<td>Optional. Disables LAND attack checks</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>option-route</td>
<td>Optional. Disables an IP Option Record Route DoS check</td>
</tr>
<tr>
<td>router-advt</td>
<td>Optional. Disables router-advt attack checks</td>
</tr>
<tr>
<td></td>
<td>This is an attack where a default route entry is added remotely to a device. This route entry is given preference, and thereby exposes a vector of attacks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| router-solicit          | Optional. Disables router-solicit attack checks  
Proto-solicitation messages are sent to locate routers as a form of network scanning. This information can then be used to attack a device.          |
| smurf                   | Optional. Disables smurf attack checks  
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. Disables snork attack checks  
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. Disables tcp-bad-sequence checks  
This DoS attack uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network of a specific TCP connection. Disables tcp-bad-sequence check. |
| tcp-fin-scan            | Optional. Disables TCP FIN scan checks  
A FIN scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.                                                                                           |
| tcp-intercept           | Optional. Disables TCP intercept attack checks  
Prevents TCP intercept attacks by using TCP SYN cookies.                                                                                                                                                       |
| tcp-null-scan           | Optional. Disables TCP Null scan checks  
A TCP null scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.                                                                                         |
| tcp-post-syn            | Optional. Disables TCP post SYN DoS attack checks                                                                                                                                                            |
| tcp-sequence-past-window| Optional. Disables TCP SEQUENCE PAST WINDOW DoS attack checks  
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.                                                                          |
| tcp-xmas-scan           | Optional. Disables TCP XMAS scan checks  
A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.                                                                                         |
| tcphdrfrag              | Optional. Disables TCP header checks  
A DoS attack where the TCP header spans IP fragments.                                                                                                                                                           |
| twinge                  | Optional. Disables twinge attack checks  
A twinge attack is a flood of false ICMP packets to try and slow down a system.                                                                                                                                 |
| udp-short-hdr           | Optional. Disables UDP short header checks  
Enables the identification of truncated UDP headers and UDP header length fields.                                                                                                                             |
| winnuke                 | Optional. Disables Winnuke checks  
This DoS attack is specific to Windows™ 95 and Windows™ NT, causing devices to crash with a blue screen.                                                                                                       |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ip tcp</td>
<td>Identifies and disables TCP events and configuration items</td>
</tr>
<tr>
<td>adjust-mss</td>
<td>Disables the adjust MSS configuration</td>
</tr>
<tr>
<td>optimize-unnecessary-resends</td>
<td>Disables the validation of unnecessary TCP packets</td>
</tr>
<tr>
<td>recreate-flow-on-out-of-state-sync</td>
<td>Disallows 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>Disables the sequence number validation in ICMP unreachable error packets</td>
</tr>
<tr>
<td>validate-rst-ack-number</td>
<td>Disables the acknowledgment number validation in RST packets</td>
</tr>
<tr>
<td>validate-rst-seq-number</td>
<td>Disables the sequence number validation in RST packets</td>
</tr>
<tr>
<td>no ip-mac conflict</td>
<td>Disables IP MAC configuration</td>
</tr>
<tr>
<td>conflict</td>
<td>Disables the action performed when a conflict exists between the IP address and MAC address</td>
</tr>
<tr>
<td>no ip-mac routing conflict</td>
<td>Disables IP MAC configuration</td>
</tr>
<tr>
<td>routing</td>
<td>Configures a routing table based action</td>
</tr>
<tr>
<td>conflict</td>
<td>Disables the action performed when a conflict exists in the routing table</td>
</tr>
<tr>
<td>no logging</td>
<td>Disables enhanced firewall logging</td>
</tr>
<tr>
<td>icmp-packet-drop</td>
<td>Disables dropping of ICMP packets that do not pass sanity checks</td>
</tr>
<tr>
<td>malformed-packet-drop</td>
<td>Disables dropping of raw IP packets that do not pass sanity checks</td>
</tr>
<tr>
<td>verbose</td>
<td>Disables verbose logging</td>
</tr>
<tr>
<td>no storm-control</td>
<td>Disables storm control</td>
</tr>
<tr>
<td>arp</td>
<td>Disables storm control for ARP packets</td>
</tr>
<tr>
<td>broadcast</td>
<td>Disables storm control for broadcast packets</td>
</tr>
<tr>
<td>multicast</td>
<td>Disables storm control for multicast packets</td>
</tr>
<tr>
<td>unicast</td>
<td>Disables storm control for unicast packets</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fe &lt;1-4&gt;</td>
<td>Disables the FastEthernet port</td>
</tr>
<tr>
<td>ge &lt;1-8&gt;</td>
<td>Disables the Gigabit Ethernet port</td>
</tr>
<tr>
<td>no virtual-defragmentation</td>
<td>Disables the virtual defragmentation of IPv4 packets</td>
</tr>
<tr>
<td>maximum-defragmentation-per-host &lt;1-16384&gt;</td>
<td>Optional. Disables the maximum active IPv4 defragmentation per host</td>
</tr>
<tr>
<td>maximum-fragments-per-datagram &lt;2-8129&gt;</td>
<td>Optional. Disables the maximum IPv4 fragments per datagram</td>
</tr>
<tr>
<td>minimum-first-fragment-length &lt;8-1500&gt;</td>
<td>Optional. Disables the minimum length required for the first IPv4 fragment</td>
</tr>
</tbody>
</table>

**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)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-logging</td>
<td>Enables logging on flow creating traffic</td>
</tr>
<tr>
<td>alg</td>
<td>Configures algorithms used with a firewall policy</td>
</tr>
<tr>
<td>clamp</td>
<td>Limits the TCP MSS to the MTU value of the inner protocol for tunneled packets</td>
</tr>
<tr>
<td>dhcp-offer-convert</td>
<td>Enables the conversion of broadcast DHCP offer packets to unicast</td>
</tr>
<tr>
<td>dns-snoop</td>
<td>Configures the DNS snoop table entry timeout</td>
</tr>
<tr>
<td>firewall</td>
<td>Enables firewalls</td>
</tr>
<tr>
<td>flow</td>
<td>Configures firewall flows</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP settings</td>
</tr>
<tr>
<td>ip-mac</td>
<td>Defines actions based on the device IP MAC table</td>
</tr>
<tr>
<td>logging</td>
<td>Configures firewall logging</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>Enables the generation of ARP responses on behalf of other devices</td>
</tr>
</tbody>
</table>
| stateful-packet-
  inspection-12       | Enables layer 2 stateful packet inspection                                   |
| storm-control        | Configures storm control                                                     |
| virtual-defragmentation | Configures the virtual defragmentation of packets at the firewall level   |
13.1.12 proxy-arp

Enables the generation of ARP responses on behalf of another device. This option is enabled by default. Supported in the following platforms:

- Access Points — AP300, 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, 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>
13.1.13 stateful-packet-inspection-l2

*firewall-policy*

Enables layer 2 firewall stateful packet inspection. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP300, 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, 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><code>no</code></td>
<td>Disables stateful packet inspection in a layer 2 firewall</td>
</tr>
</tbody>
</table>
13.1.14 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
storm-control [arp|broadcast|multicast|unicast] level <1-1000000> [fe <1-4>|ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]
```

```
storm-control [arp|broadcast|multicast|unicast] log [<0-7>|alerts|critical|debugging|emergencies|errors|informational|none|notifications|warnings]
```

Parameters

- storm-control [arp|broadcast|multicast|unicast] level <1-1000000> [fe <1-4]|ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]

<table>
<thead>
<tr>
<th>Parameter</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>level &lt;1-1000000&gt;</td>
<td>Configures the allowed number of packets received per second before storm control begins</td>
</tr>
<tr>
<td>fe &lt;1-4&gt;</td>
<td>Sets the FastEthernet port for storm control from 1 - 4</td>
</tr>
<tr>
<td>ge &lt;1-8&gt;</td>
<td>Sets the GigabitEthernet port for storm control from 1 - 8</td>
</tr>
<tr>
<td>port-channel &lt;1-8&gt;</td>
<td>Sets the port channel for storm control from 1- 8</td>
</tr>
<tr>
<td>up1</td>
<td>Sets the uplink interface</td>
</tr>
<tr>
<td>wlan &lt;WLAN-NAME&gt;</td>
<td>Configures the WLAN</td>
</tr>
</tbody>
</table>

Note: For the NX45XX and NX65XX service platforms, the GE port range is 1 - 24.

Note: For the NX45XX and NX65XX service platforms, the uplink interface range is 1 - 2.

Note: <WLAN-NAME> — Sets the WLAN ID for the storm control configuration
FIREWALL-POLICY 13 - 35

- 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
13.1.15 virtual-defragmentation

```
firewall-policy
```

Enables virtual defragmentation of IPv4 packets. This parameter is required for optimal firewall functionality and is enabled by default.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX6500, NX6524, NX7500, 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>}
```

**Parameters**

- `virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum-defragmentation-per-host &lt;1-16384&gt;</td>
<td>Optional. Defines the maximum active IPv4 defragmentation per host</td>
</tr>
<tr>
<td>maximum-fragments-per-datagram &lt;2-8129&gt;</td>
<td>Optional. Defines the maximum IPv4 fragments per datagram (for virtual defragmentation)</td>
</tr>
<tr>
<td>minimum-first-fragment-length &lt;8-1500&gt;</td>
<td>Optional. Defines the minimum length required for the first IPv4 fragment (for virtual defragmentation)</td>
</tr>
</tbody>
</table>

**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
rfs7000-37FABE(config-fw-policy-test)#
```

**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)#
```
15.1 mint-policy

Table 15.1 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 15-3</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the global MiNT MTU</td>
<td>page 15-4</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 15-7</td>
</tr>
<tr>
<td>router</td>
<td>Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)</td>
<td>page 15-5</td>
</tr>
<tr>
<td>udp</td>
<td>Configures the MiNT UDP/IP encapsulation parameters</td>
<td>page 15-6</td>
</tr>
</tbody>
</table>
15.1.1 level

Configures the global MiNT routing level

Supported in the following platforms:
- Access Points — AP300, 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, 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)
15.1.2 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
mtu <900-1500>
```

**Parameters**

- `mtu <900-1500>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;900-1500&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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
15.1.3 router

`mint-policy`

Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

`router packet priority <0-7>`

Parameters

- `router packet priority <0-7>`

| router packet priority <0-7> | Allows you to configure the priority for MiNT router packets from 0 - 7. The default is 5. **Note:** Higher the value higher is the priority. Therefore, seven (7) represents highest priority. |

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

- `no` Reverts the MiNT router packet priority to default (5)
15.1.4 **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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`udp port <2-65534>`

**Parameters**

- `udp port <2-65534>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;2-65534&gt;</td>
<td>Configures default UDP port used for MiNT control packet encapsulation</td>
</tr>
</tbody>
</table>

- `<2-65534>` – Enter a value from 2 - 65534. This value specifies an alternate UDP port used by MiNT control packets and must be an even number. The specified port number plus 1 is used to carry MiNT data packets. The default value is 24576.

**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
```

**Related Commands**

- `no` Reverts MiNT UDP/IP encapsulation to its default
15.1.5 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
no [level|mtu|router|udp]
no level 2 area-id
no mtu
no router packet priority
no udp port <LINE-SINK>

Parameters
- no level 2 area-id
  - no level 2
    - Disables level 2 MiNT routing
  - area identifier
    - Negates the area identifier
- no mtu
  - no mtu
    - Reverts the configured MiNT MTU value to its default
- no router packet priority
  - no router packet priority
    - Resets the MiNT router packet priority to default
- no udp port <LINE-SINK>
  - no udp
    - Resets the UDP/IP encapsulation parameters to its default
  - port <LINE-SINK>
    - Uses the default UDP port for MiNT encapsulation

Examples
The following example shows the global Mint Policy parameters before the ‘no’ commands are executed:

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)#
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

The following example shows the global Mint Policy parameters after the `no` commands are executed:

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)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Configures the global MiNT routing level</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the global MiNT MTU</td>
</tr>
<tr>
<td>router</td>
<td>Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)</td>
</tr>
<tr>
<td>udp</td>
<td>Configures the MiNT UDP/IP encapsulation parameters</td>
</tr>
</tbody>
</table>
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 uaccess 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>

rfs7000-37FABE(config)#management-policy test
To commit a management-policy, at least one admin user account must always be present in the management-policy:

```
rfs7000-37FABE(config-management-policy-test)#user admin password 0 admin123 role superuser access all
rfs7000-37FABE(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
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
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
show                     Show running system information
write                    Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-management-policy-test)#
```
### 16.1 management-policy

Table 16.1 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 16-4</td>
</tr>
<tr>
<td>banner</td>
<td>Configures the message of the day (motd) text</td>
<td>page 16-6</td>
</tr>
<tr>
<td>ftp</td>
<td>Enables FTP on this management policy</td>
<td>page 16-7</td>
</tr>
<tr>
<td>http</td>
<td>Enables HTTP on this management policy</td>
<td>page 16-9</td>
</tr>
<tr>
<td>https</td>
<td>Enables HTTPS on this management policy</td>
<td>page 16-10</td>
</tr>
<tr>
<td>idle-session-timeout</td>
<td>Sets the interval after which an idle session is terminated</td>
<td>page 16-11</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets this management policy's settings</td>
<td>page 16-12</td>
</tr>
<tr>
<td>privilege-mode-password</td>
<td>Configures the CLI's privilege mode access password</td>
<td>page 16-16</td>
</tr>
<tr>
<td>restrict-access</td>
<td>Restricts management access to a set of hosts or subnets</td>
<td>page 16-17</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Sets the SNMP server settings on this management policy</td>
<td>page 16-20</td>
</tr>
<tr>
<td>ssh</td>
<td>Enables SSH on this management policy</td>
<td>page 16-25</td>
</tr>
<tr>
<td>telnet</td>
<td>Enables Telnet on this management policy</td>
<td>page 16-26</td>
</tr>
<tr>
<td>user</td>
<td>Creates a new user account</td>
<td>page 16-27</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands to troubleshoot or debug (config-if) instance configurations</td>
<td>page 16-29</td>
</tr>
</tbody>
</table>
16.1.1 aaa-login

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

aaa-login [local|radius|tacacs]

aaa-login local

aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]

aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-TACACS-POLICY-NAME>]

Parameters

- **aaa-login local**
  
  | local | Sets local as the preferred authentication mode. Local authentication uses the local username database to authenticate a user.

- **aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]**
  
  | radius | Configures the RADIUS server parameters
  | local | Sets local as the preferred authentication mode. Local authentication uses the local username database to authenticate a user.
  | 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.

- **aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-TACACS-POLICY-NAME>]**
  
  | tacacs | Configures Terminal Access Control Access-Control System (TACACS) server parameters
  | accounting | Configures TACACS accounting
  | authentication | Configures TACACS authentication
  | authorization | Configures TACACS authorization
### 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
```bash
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
- `no` Removes the TACACS server settings
16.1.2 **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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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>• <code>&lt;LINE&gt;</code> — Enter the message string. The message string should not exceed 255 characters.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
rfs7000-37FABE(config-management-policy-test)#banner motd "Have a Good Day"
```

```plaintext
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"
```

**Related Commands**

| no | Removes the motd banner |
16.1.3 ftp

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
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 [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}`
- `ftp {rootdir <DIR>}`
- `ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}`

<table>
<thead>
<tr>
<th>ftp password</th>
<th>Optional. Configures the FTP server password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 &lt;ENCRYPTED-PASSWORD&gt;</td>
<td>Configures an encrypted password. Use this option when copy pasting the password from another device.</td>
</tr>
<tr>
<td></td>
<td>• &lt;ENCRYPTED-PASSWORD&gt; – Specify the password. The password should not exceed 63 characters in length.</td>
</tr>
<tr>
<td>&lt;PASSWORD&gt;</td>
<td>Configures a clear text password</td>
</tr>
</tbody>
</table>

- `ftp {rootdir <DIR>}`

<table>
<thead>
<tr>
<th>ftp rootdir &lt;DIR&gt;</th>
<th>Optional. Configures the root directory for FTP logins</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DIR&gt;</td>
<td>Specify the root directory path. By default the root directory is set to flash:/</td>
</tr>
</tbody>
</table>

- `ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}`

<table>
<thead>
<tr>
<th>ftp username &lt;USERNAME&gt;</th>
<th>Optional. Configures a new user account on the FTP server. The FTP user file lists users with FTP server access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify the username. The username should not exceed 32 characters in length.</td>
</tr>
</tbody>
</table>

| 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 |

<table>
<thead>
<tr>
<th>rootdir &lt;DIR&gt;</th>
<th>After specifying the password, configure the FTP root directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DIR&gt;</td>
<td>Configures the root directory for FTP logins. Specify the root directory path.</td>
</tr>
</tbody>
</table>
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 admin123 rootdir dir
rfs7000-37FABE(config-management-policy-test)#show context management-policy test
http server
ftp username superuser password 1 7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
banner motd "Have a Good Day"

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>
16.1.4 http

Enables Hyper Text Transport Protocol (HTTP) on this management policy

Supported in the following platforms:
- Access Points — AP300, 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, 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
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 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
16.1.5 **https**

Enables *Hyper Text Transport Protocol Secure* (HTTPS) on this management policy. The command also allows you to enable/disable SSLv3 support.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

https [server|sslv3 enable]

**Parameters**

- https [server|sslv3 enable]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>https server</td>
<td>Enables HTTPS on this management policy. HTTPS provides both authentication and data encryption as opposed to just authentication.</td>
</tr>
<tr>
<td>https sslv3 enable</td>
<td>Enables/disables support for <em>Secure Socket Layer version 3</em> (SSLv3). SSLv3 support is enabled by default. Use the no &gt; https &gt; sslv3 command to disable SSLv3 support. Disabling SSLv3 is necessary to protect against POODLE attacks.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-management-policy-test)#https server

rfs7000-37FABE(config-management-policy-test)#show context management-policy test

http server

https server

ftp username superuser password 1

7ccb4568cb83e54fe402f785a78ee930a453afda152baaf7c2b79277f225872 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 HTTPS on this management policy. Also disables SSLv3 support.
16.1.6 idle-session-timeout

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

idle-session-timeout <1-4320>

Parameters
- idle-session-timeout <1-4320>

| <1-4320> | Sets the interval, in minutes, after which an idle session is timed out. Specify a value from 1 - 4320 minutes. The default is 30 minutes. |

Examples

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
  7cc94568cb83e54f1e402f85a78ee930a453afda152baaf7c2b79277f225872 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
16.1.7 **no**

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [aaa-login|banner|ftp|http|https|idle-session-timeout|privilege-mode-password|
restrict-access|snmp-server|ssh|telnet|user|service]

no aaa-login tacacs [accounting|authentication|authorization|fallback|policy]

no banner motd

no ftp {password|rootdir}

no http server

no https [server|sslv3]

no [idle-session-timeout|privilege-mode-password|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 [telnet|user <USERNAME>]

no service prompt crash-info
```

**Parameters**

- **no aaa-login tacacs** [accounting|authentication|authorization|fallback|policy]

| no aaa-login | Disables or reverts user authorization parameters |
| tacacs       | Disables the TACACS server parameters            |
| accounting   | Disables TACACS accounting                       |
| authentication| Disables TACACS authentication                   |
| authorization | Disables TACACS authorization                    |
| fallback     | Disables TACACS as the primary authentication mode|
| policy       | Disassociates a specified TACACS policy from this management policy |
- **no banner motd**

  no banner motd  
  Removes the motd banner

- **no ftp {password|rootdir}**

  no ftp  
  Reverts to default FTP server settings

  password  
  Optional. Reverts to default FTP password

  rootdir  
  Optional. Reverts to default FTP root directory

- **no http server**

  no http  
  Disables the HTTP server on this management policy

  no https  
  Disables the HTTPS server on this management policy

- **no https server**

  no https server  
  Disables the HTTPS server on this management policy

  no https sslv3  
  Disables SSLv3 support on this management policy

- **no [idle-session-timeout|privilege-mode-password|restrict-access]**

  no idle-session-timeout  
  Disables a defined session timeout interval

  no privilege-mode-password  
  Removes the configured CLI privilege mode access password

  no restrict-session  
  Removes management access restrictions on this management policy

- **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 snmp-server  
  Disables the SNMP server parameters

  community <WORD>  
  Disables SNMP server access to a community

  - `<WORD>` – Specify the community name.

  display-vlan-info-per-radio  
  Disables the display of the VLAN ID along with the radio interface ID (only displays the radio interface)

  enable traps  
  Disables SNMP traps

  host <IP> {<1-65535>}

  - Removes SNMP host (trap recipient) details

  - `<IP>` – Specify the host’s IP address.

  - `<1-65535>` – Optional. Resets the port for receiving SNMP traps to default (162)

  manager [all|v1|v2|v3]  
  Disables SNMP manager

  max-pending-requests  
  Resets the maximum pending requests to default (128)

  request-timeout  
  Resets the request timeout to default (240 seconds)
### 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
  7ccb45b8cb3e54f1e02f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
  no ssh
  aaa-login radius external
  idle-session-timeout 100
  banner motd "Have a Good Day"
```

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

```
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:

```plaintext
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
no http server
https server
ftp username superuser password 1
626b4033263d6d2ae4e79c48cdefcccb60fd4c77a8da9e365060594a6d570ec2 rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 0
rfs7000-37FABE(config-management-policy-test)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa-login</td>
<td>Configures the AAA authentication mode used with this management policy</td>
</tr>
<tr>
<td>banner</td>
<td>Configures the login motd banner</td>
</tr>
<tr>
<td>ftp</td>
<td>Configures the FTP server parameters</td>
</tr>
<tr>
<td>http</td>
<td>Enables HTTP</td>
</tr>
<tr>
<td>https</td>
<td>Enables HTTPS</td>
</tr>
<tr>
<td>idle-session-timeout</td>
<td>Configures a session's idle timeout</td>
</tr>
<tr>
<td>privilege-mode-password</td>
<td>Configures the CLI's privilege mode access password</td>
</tr>
<tr>
<td>restrict-access</td>
<td>Restricts management access to a set of hosts or subnets. Also enables the logging of access requests</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Configures SNMP engine parameters</td>
</tr>
<tr>
<td>ssh</td>
<td>Enables a SSH connection between client and server</td>
</tr>
<tr>
<td>telnet</td>
<td>Enables Telnet</td>
</tr>
<tr>
<td>user</td>
<td>Adds a new user account</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands to troubleshoot or debug (config-if) instance configurations</td>
</tr>
</tbody>
</table>
16.1.8 privilege-mode-password

Configures the CLI’s privilege mode access password

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
privilege-mode-password [1 <PASSWORD>|<PASSWORD>]
```

Parameters

```
privilege-mode-password [1 <PASSWORD>|<PASSWORD>]
```

<table>
<thead>
<tr>
<th>1 &lt;PASSWORD&gt;</th>
<th>Configures an encrypted password. Use this option when copy pasting the password from another device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PASSWORD&gt;</td>
<td>Configures a clear text password</td>
</tr>
</tbody>
</table>

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 2e9f038ac2ed27f919ed5a4dceb3d30e32f356f2ceff6f6b26a153d0339c734f
```
```
rfs7000-37FABE(config-management-policy-test)#
```

Related Commands

```
no
```

Removes the configured CLI privilege mode access password
### 16.1.9 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restrict-access [host</td>
<td>ip-access-list</td>
</tr>
<tr>
<td>restrict-access host &lt;IP&gt; {&lt;IP&gt;</td>
<td>log [all</td>
</tr>
<tr>
<td>restrict-access host &lt;IP&gt; {&lt;IP&gt;</td>
<td>log [all</td>
</tr>
<tr>
<td>restrict-access ip-access-list &lt;IP-ACCESS-LIST-NAME&gt;</td>
<td>Restricts access to the host on a specified subnet. Uses the IP address of a host to filter access requests.</td>
</tr>
<tr>
<td>restrict-access subnet &lt;IP/M&gt; {&lt;IP/M&gt;</td>
<td>host</td>
</tr>
<tr>
<td>restrict-access subnet &lt;IP/M&gt; {&lt;IP/M&gt;</td>
<td>log [all</td>
</tr>
<tr>
<td>restrict-access subnet &lt;IP/M&gt; {&lt;IP/M&gt;</td>
<td>log [all</td>
</tr>
<tr>
<td>restrict-access subnet &lt;IP/M&gt; {&lt;IP/M&gt;</td>
<td>log [all</td>
</tr>
</tbody>
</table>

**Parameters**

- **host <IP>**
  - Restricts management access to a specified host. Filters access requests based on a host's IP address.
  - `<IP>` – Specify the host's IP address.

- **<IP>**
  - Optional. Use this option to add multiple hosts, if required, to the restrict access list.

- **log [all|denied-only]**
  - Optional. Configures a logging policy for access requests. Sets the log type generated for access requests.
  - `all` – Logs all access requests, both denied and permitted.
  - `denied-only` – Logs only denied access (when an access request is received from a host denied access, a record is logged).
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP/M&gt;</code></td>
<td>Optional. Use this option to add multiple subnets, if required, to the restrict access list.</td>
</tr>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
<tr>
<td></td>
<td>• all – Logs all access requests, both denied and permitted</td>
</tr>
<tr>
<td></td>
<td>• denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)</td>
</tr>
<tr>
<td>restrict-access ip-access-list</td>
<td>Uses an IP access list to filter access requests.</td>
</tr>
<tr>
<td>ip-access-list</td>
<td>IP based firewalls function like Access Control Lists (ACLs) to filter/mark packets based on the IP from which they arrive, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies. To have effective firewalls, you need to have a clear idea of the kind of access to allow or deny. A poorly defined firewall is of little value, and could provide a false sense of network security.</td>
</tr>
<tr>
<td><code>&lt;IP-ACCESS-LIST-NAME&gt;</code></td>
<td>Sets the access list name</td>
</tr>
<tr>
<td>restrict-access subnet <code>&lt;IP/M&gt;</code></td>
<td>Restricts access to a specified subnet. Uses a subnet IP address to filter access requests.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP/M&gt;</code> – Sets the IP address of the subnet in the A.B.C.D/M format</td>
</tr>
<tr>
<td><code>&lt;IP/M&gt;</code></td>
<td>Optional. Use this option to add multiple subnets, if required, to the restrict access list.</td>
</tr>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
<tr>
<td></td>
<td>• all – Logs all access requests, both denied and permitted</td>
</tr>
<tr>
<td></td>
<td>• denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)</td>
</tr>
<tr>
<td>restrict-access subnet <code>&lt;IP/M&gt;</code></td>
<td>Restricts access to a specified subnet. Uses a subnet IP address to filter access requests.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP/M&gt;</code> – Sets the IP address of the subnet in the A.B.C.D/M format</td>
</tr>
<tr>
<td>host <code>&lt;IP&gt;</code></td>
<td>Uses the host IP address as a second filter</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;IP&gt;</code> – Specify the host IP address.</td>
</tr>
<tr>
<td>log [all</td>
<td>denied-only]</td>
</tr>
<tr>
<td></td>
<td>• all – Logs all access requests, both denied and permitted</td>
</tr>
<tr>
<td></td>
<td>• denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)</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 626b4033263d6d2ae4e79c48cdefc0b60fd4c77a8da9e365060597a6d6570ec2 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
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 device access restrictions</td>
</tr>
</tbody>
</table>
16.1.10 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 — AP300, 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, 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]

snmp-server enable traps

snmp-server host <IP> [v2c|v3] {<1-65535>|community}

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|snmpprop]

snmp-server user [snmpmanager|snmpoperator|snmpprop] v3 [auth|encrypted]

snmp-server user [snmpmanager|snmpoperator|snmpprop] v3 auth md5
  [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]

snmp-server user [snmpmanager|snmpoperator|snmpprop] v3 encrypted
  [auth md5|des auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

Parameters

- `snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw]`

| community [0 <WORD>|2 <WORD>|<WORD>] | 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 Configuration

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server enable traps</strong></td>
</tr>
<tr>
<td><strong>enable traps</strong> 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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>**snmp-server host &lt;IP&gt; [v2c</td>
</tr>
<tr>
<td>host &lt;IP&gt; Configures a host's IP address. This is the external server resource dedicated to receiving SNMP traps on behalf of the controller.</td>
</tr>
<tr>
<td>[v2c</td>
</tr>
<tr>
<td>• v2c – Uses SNMP version 2c</td>
</tr>
<tr>
<td>• v3 – Uses SNMP version 3</td>
</tr>
<tr>
<td>&lt;1-65535&gt; Optional. Specifies the host's UDP port number. This is port used by the external resource to receive SNMP traps.</td>
</tr>
<tr>
<td>• &lt;1-65535&gt; – Optional. Sets a value from 1 - 65535. The default port is 162.</td>
</tr>
<tr>
<td>community Specify the SNMP trap community name. The default value is public.</td>
</tr>
<tr>
<td>**snmp-server manager [all</td>
</tr>
<tr>
<td>manager [all</td>
</tr>
<tr>
<td>• all – Enables SNMP manager version 2 and v3</td>
</tr>
<tr>
<td>• 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.</td>
</tr>
<tr>
<td>• 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.</td>
</tr>
<tr>
<td>• v3 – Enables SNMP manager version v3 only. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the <strong>User-based Security Model (USM)</strong> for message security and the <strong>View-based Access Control Model (VACM)</strong> for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.</td>
</tr>
</tbody>
</table>
### snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]

<table>
<thead>
<tr>
<th>max-pending-requests {&lt;64-1024&gt;}</th>
<th>Sets the maximum number of requests that can be pending at any given time</th>
</tr>
</thead>
<tbody>
<tr>
<td>{&lt;64-1024&gt;} – Optional. Specify a value from 64 - 1024. The default is 128.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>request-timeout {&lt;2-720&gt;}</th>
<th>Sets the interval, in seconds, after which an error message is returned for a pending request</th>
</tr>
</thead>
<tbody>
<tr>
<td>{&lt;2-720&gt;} – Optional. Specify a value from 2 - 720 seconds. The default is 240 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

### snmp-server [display-vlan-info-per-radio|throttle <1-100>|suppress-security-configuration-level [0|1]]

<table>
<thead>
<tr>
<th>display-vlan-info-per-radio</th>
<th>Enables the display of the VLAN ID along with the radio interface ID</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>throttle &lt;1-100&gt;</th>
<th>Sets CPU usage for SNMP activities. Use this command to set the CPU usage from 1 - 100.</th>
</tr>
</thead>
</table>

| 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 |

<table>
<thead>
<tr>
<th>v3 auth md5</th>
<th>Uses SNMP version 3 as the security model</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth – Uses an authentication protocol</td>
<td></td>
</tr>
<tr>
<td>md5 – Uses HMAC-MD5 algorithm for authentication</td>
<td></td>
</tr>
</tbody>
</table>

| [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>] | Configures password using one of the following options: |
|------------------------------------------------|---------------------------------------------------------------------|
| 0 <PASSWORD> – Configures clear text password |
| 2 <PASSWORD> – Configures encrypted password |
| <PASSWORD> – Specifies a password for authentication and privacy protocols |
### SNMP Server Configuration

- **snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted [auth md5|des auth md5] [0 <PASSWORD> 2 <ENCRYPTED-PASSWORD>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Defines user access to the SNMP engine</td>
</tr>
<tr>
<td>[snmpmanager</td>
<td>snmpoperator</td>
</tr>
<tr>
<td></td>
<td>- snmpoperator – Sets user as a SNMP operator</td>
</tr>
<tr>
<td></td>
<td>- snmptrap – Sets user as a SNMP trap user</td>
</tr>
<tr>
<td>v3 encrypted</td>
<td>Uses SNMP version 3 as the security model</td>
</tr>
<tr>
<td>auth md5</td>
<td>Uses authentication protocol</td>
</tr>
<tr>
<td></td>
<td>- auth – Sets authentication parameters</td>
</tr>
<tr>
<td></td>
<td>- md5 – Uses HMAC-MD5 algorithm for authentication</td>
</tr>
<tr>
<td>des auth md5</td>
<td>Uses privacy protocol for user privacy</td>
</tr>
<tr>
<td></td>
<td>- des – Uses CBC-DES for privacy</td>
</tr>
<tr>
<td></td>
<td>After specifying the privacy protocol, specify the authentication mode.</td>
</tr>
<tr>
<td></td>
<td>- auth – Sets user authentication parameters</td>
</tr>
<tr>
<td></td>
<td>- md5 – Uses HMAC-MD5 algorithm for authentication</td>
</tr>
<tr>
<td>[0 &lt;PASSWORD&gt;] 2 &lt;ENCRYPTED-PASSWORD&gt;</td>
<td>The following are common to both the auth and des parameters:</td>
</tr>
<tr>
<td></td>
<td>Configures password using one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- 0 &lt;PASSWORD&gt; – Configures a clear text password</td>
</tr>
<tr>
<td></td>
<td>- 2 &lt;PASSWORD&gt; – Configures an encrypted password</td>
</tr>
<tr>
<td></td>
<td>- &lt;PASSWORD&gt; – Specifies a password for authentication and privacy protocols</td>
</tr>
</tbody>
</table>

#### Examples

```bash
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 admin123
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
no http server
https server
ftp username superuser password 1
626b4033263d6d2ae4e79c48cfdcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
no ssh
snmp-server community snmp1 ro
snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
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)#
```

```bash
rfs7000-1A45FE(config-management-policy-default)#snmp-server host 192.168.1.2 v2c 1000
rfs7000-1A45FE(config-management-policy-default)#snmp-server host 192.168.1.2 v2c community ?
rfs7000-1A45FE(config-management-policy-default)#snmp-server host 192.168.1.2 v2c community test1234
```
rfs7000-1A45FE(config-management-policy-default)#commit write
rfs7000-1A45FE(config-management-policy-default)#snmp-server host 192.168.1.2 v2c 3000 community 12341234123412341234123412341234
rfs7000-1A45FE(config-management-policy-default)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables or resets the SNMP server settings</td>
</tr>
</tbody>
</table>
16.11 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>Parameter</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></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
  626b403263d6d2ae4e79c482dfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
  ssh port 162
  snmp-server community snmp1 ro
  snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
  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

no | Resets SSH access port to factory default (port 22)
16.1.12 telnet

Enables 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 — AP300, 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, 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><code>telnet</code></td>
<td>Enables Telnet</td>
</tr>
<tr>
<td><code>port &lt;1-65535&gt;</code></td>
<td>Optional. Configures the Telnet port. This is the port used for Telnet connections. It sets a value from 1 - 165535. 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
  626b4033263dd2ae4e79c48cdfe8c60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
  ssh port 162
  snmp-server community snmp1 ro
  snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
  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

- `no` Disables Telnet
### 16.1.13 user

**management-policy**

Adds new user account

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>]
role [helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin] access [all|console|ssh|telnet|web]
```

**Parameters**

- `user <USERNAME>` – Adds new user account to this management policy
  - `<USERNAME>` – Sets the username

- `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

- `role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]` – Configures the user role. The options are:
  - `device-provisioning-admin` – Device provisioning administrator.
  - `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.
  - `monitor` – Monitor. Has read-only access to the system. Can view configuration and statistics except for secret information
  - `network-admin` – Network administrator. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF
  - `security-admin` – Security administrator. 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.
### access

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`all</td>
<td>console</td>
</tr>
<tr>
<td>• <code>all</code> – Allows all types of access: console, SSH, Telnet, and Web</td>
<td></td>
</tr>
<tr>
<td>• <code>console</code> – Allows console access only</td>
<td></td>
</tr>
<tr>
<td>• <code>ssh</code> – Allows SSH access only</td>
<td></td>
</tr>
<tr>
<td>• <code>telnet</code> – Allows Telnet access only</td>
<td></td>
</tr>
<tr>
<td>• <code>web</code> – Allows Web access only</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

```
access [all|console|ssh|telnet|web]

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 626b4033263d6d2ae4e79c48cddfcccbb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
ssh port 162
user TESTER password 1 737670e898600bcc42ee91aab93b568efa73ffee5f4d1e1b12262887ac3646bc
role superuser access all
snmp-server community snmp1 ro
snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
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

<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>
16.1.14 service

Invokes service commands

Supported in the following platforms:

- **Access Points** — AP300, 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, 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</th>
<th>Updates CLI prompt settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>crash-info</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)]
      + 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
```

**Related Commands**

- `no`
  - Disables the inclusion of an asterix indicator notifying the presence of crash files
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
17.1 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
<rfs7000-37FABE>(config)#radius-group <GROUP-NAME>
```

Example:
```
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

```
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.
Table 17.1 summarizes RADIUS group configuration commands.

**Table 17.1 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 17-4</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 17-10</td>
</tr>
<tr>
<td>policy</td>
<td>Configures RADIUS group access policy parameters</td>
<td>page 17-5</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 17-9</td>
</tr>
</tbody>
</table>
17.1.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

guest

Parameters

None

Examples

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

no

Makes this group a non-guest group
17.1.2 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

policy [access|day|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 role [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 [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:  
- 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 ssid <SSID>  

**ssid <SSID>**  
Sets the Service Set Identifier (SSID) for this guest RADIUS group. Use this command to assign SSIDs that users within this RADIUS group are allowed to associate. Assign SSIDs of those WLANs only that the guest users need to access. This option is not available for a management group.  
- <SSID> – Sets a case-sensitive alphanumeric SSID, not exceeding 32 characters
### RADIUS-POLICY

**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:

```plaintext
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:

```plaintext
```

---

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
</table>
| **policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|weekdays)}** | Configures the days on which this guest RADIUS group members can access the local RADIUS resources. The options are recursive, and you can provide access on multiple days.  
  - fr – Allows access on Friday only  
  - mo – Allows access on Mondays only  
  - sa – Allows access on Saturdays only  
  - su – Allows access on Sundays only  
  - th – Allows access on Thursdays only  
  - tu – Allows access on Tuesdays only  
  - we – Allows access on Wednesdays only  
  - weekdays – Allows access on weekdays only (Monday to Friday) |
| **policy time start <HH:MM> end <HH:MM>** | Configures the time when this RADIUS group can access the network  
  - start <HH:MM> – Sets the start time in the HH:MM format (for example, 13:30 means the user can login only after 1:30 PM). Specifies the time users, within each listed group, can access the local RADIUS resources  
  - end <HH:MM> – Sets the end time in the HH:MM format (for example, 17:30 means the user is allowed to remain logged in until 5:30 PM). Specifies the time users, within each listed group, lose access to the local RADIUS resources |
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 |
17.1.3 rate-limit

Sets the rate limit for the guest RADIUS server group

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

rate-limit [from-air|to-air] <100-1000000>

---

**NOTE:** The rate-limit setting is not applicable to a management group.

Parameters

- rate-limit [from-air|to-air] <100-1000000>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>to-air &lt;100-1000000&gt;</td>
<td>Sets the rate limit in the downlink direction, from the network to the wireless client</td>
</tr>
<tr>
<td>&lt;100-1000000&gt;</td>
<td>Sets the rate from 100 - 1000000 Kbps</td>
</tr>
<tr>
<td>from-air &lt;100-1000000&gt;</td>
<td>Sets the rate limit in the uplink direction, from the wireless client to the network</td>
</tr>
<tr>
<td>&lt;100-1000000&gt;</td>
<td>Sets the rate from 100 - 1000000 Kbps</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-radius-group-test)##rate-limit to-air 101
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
17.1.4 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [guest|policy|rate-limit]

no policy [access|day|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 [role|time|vlan]

no rate-limit [from-air|to-air]

Parameters

- no guest

<table>
<thead>
<tr>
<th>no guest</th>
<th>Makes a RADIUS guest group a non-guest (management) group</th>
</tr>
</thead>
</table>

- no policy access [all|console|ssh|telnet|web]

<table>
<thead>
<tr>
<th>no policy access</th>
<th>Removes or modifies the RADIUS management group access</th>
</tr>
</thead>
<tbody>
<tr>
<td>all – Removes all access (Wireless client access to the console, SSH, Telnet, and Web)</td>
<td></td>
</tr>
<tr>
<td>console – Removes console access</td>
<td></td>
</tr>
<tr>
<td>ssh – Removes SSH access</td>
<td></td>
</tr>
<tr>
<td>telnet – Removes Telnet</td>
<td></td>
</tr>
<tr>
<td>web – Removes Web access</td>
<td></td>
</tr>
</tbody>
</table>

These are recursive options, and you can remove more than one at a time.

- no policy day [all|fr|mo|sa|su|th|tu|we|weekdays]

<table>
<thead>
<tr>
<th>no policy days</th>
<th>Removes or modifies the days on which access is provided to a RADIUS guest group</th>
</tr>
</thead>
<tbody>
<tr>
<td>all – Removes access on all days (Monday to Sunday)</td>
<td></td>
</tr>
<tr>
<td>fr – Removes access on Fridays only</td>
<td></td>
</tr>
<tr>
<td>mo – Removes access on Mondays only</td>
<td></td>
</tr>
<tr>
<td>sa – Removes access on Saturdays only</td>
<td></td>
</tr>
<tr>
<td>su – Removes access on Sundays only</td>
<td></td>
</tr>
<tr>
<td>th – Removes access on Thursdays only</td>
<td></td>
</tr>
<tr>
<td>tu – Removes access on Tuesdays only</td>
<td></td>
</tr>
</tbody>
</table>

Contd..
### RADIUS-POLICY 17 - 11

#### Examples

The following example shows the RADIUS guest group ‘test’ settings before the ‘no’ commands are executed:

```plaintext
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)#
```

The following example shows the RADIUS guest group ‘test’ settings after the ‘no’ commands are executed:

```plaintext
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)#
```

---

### RADIUS-POLICY 17 - 11

- **we** – Removes access on Wednesdays only
- **weekdays** – Removes access on weekdays (Monday to Friday)

These are recursive options, and you can remove more than one at a time.

---

#### no policy ssid `<SSID>|all`

- **no policy ssid** Removes a SSID assigned to a RADIUS guest group
  - `<SSID>` – Specify the RADIUS group SSID. RADIUS group users will not be allowed access to the WLAN represented by the specified SSID.
  - **all** – Removes all allowed WLANs

---

#### no policy [role|time|vlan]

- **no policy role** Removes the RADIUS management group’s role
- **no policy time** Removes the RADIUS guest group’s start and end access time
- **no policy vlan** Removes the RADIUS guest group’s VLAN ID

---

#### no rate-limit [from-air|to-air]

- **no rate-limit** Removes RADIUS guest group’s rate limit
  - **from-air** Removes the uplink (from wireless client to network) rate limit
  - **to-air** Removes the downlink (from network to wireless client) rate limit
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest</td>
<td>Manages a guest user linked with a captive portal</td>
</tr>
<tr>
<td>policy</td>
<td>Sets a RADIUS group’s authorization policies</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Sets a RADIUS group’s rate limit</td>
</tr>
</tbody>
</table>
### 17.2 radius-server-policy

**RADIUS-POLICY**

Creates an onboard device RADIUS server policy.

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:

```text
<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
- **chase-referral**
  - Enables LDAP server referral chasing
- **crl-check**
  - Enables Certificate Revocation List (CRL) check
- **ldap-agent**
  - Configures the LDAP agent’s settings
- **ldap-group-verification**
  - Enables 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**
  - Enables session resumption/fast reauthentication by using cached attributes
- **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)#`

| Table 17.2 summarizes RADIUS server policy configuration commands. |
| --- | --- | --- |
| **Commands** | **Description** | **Reference** |
| **authentication** | Configures RADIUS authentication settings | page 17-15 |
| **chase-referral** | Enables LDAP server referral chasing | page 17-17 |
| **crl-check** | Enables a certificate revocation list (CRL) check | page 17-18 |
| **ldap-agent** | Configures the LDAP agent’s settings | page 17-19 |
### Table 17.2 RADIUS-Server-Policy-Config Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-group-verification</td>
<td>Enables LDAP group verification</td>
<td>page 17-21</td>
</tr>
<tr>
<td>ldap-server</td>
<td>Configures the LDAP server’s settings</td>
<td>page 17-22</td>
</tr>
<tr>
<td>local</td>
<td>Configures a local RADIUS realm</td>
<td>page 17-25</td>
</tr>
<tr>
<td>nas</td>
<td>Configures the key sent to a RADIUS client</td>
<td>page 17-26</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets the RADIUS server policy’s settings</td>
<td>page 17-27</td>
</tr>
<tr>
<td>proxy</td>
<td>Configures the RADIUS proxy server’s settings</td>
<td>page 17-31</td>
</tr>
<tr>
<td>session-resumption</td>
<td>Enables session resumption</td>
<td>page 17-33</td>
</tr>
<tr>
<td>use</td>
<td>Defines settings used with the RADIUS server policy</td>
<td>page 17-34</td>
</tr>
</tbody>
</table>
17.2.1 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
authentication [data-source|eap-auth-type]
```

<table>
<thead>
<tr>
<th>data-source</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ldap</strong></td>
<td>Uses a remote LDAP server as the data source</td>
</tr>
<tr>
<td><strong>local</strong></td>
<td>Uses the local user database to authenticate a user</td>
</tr>
</tbody>
</table>
| **ssid <SSID>** precedence <1-5000> | The following keywords are recursive and common to both ‘ldap’ and ‘local’ parameters: |}
| **<SSID>**                         | • ssid – Optional. Associates the data source, selected in the previous step, with a SSID. |
| **precedence <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. |
| **eap-auth-type**                 | Uses Extensible Authentication Protocol (EAP), with this RADIUS server policy, for user authentication |
| **all**                           | The EAP authentication types supported by the local RADIUS server are: all, peap-gtc, peap-mschapv2, tls, ttls-md5, ttls-mschapv2, ttls-pap. |

**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.
- The default setting is local.

- 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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables both TTLS and PEAP authentication</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**

```bash
rfs7000-37FABE(config-radius-server-policy-test)#authentication eap-auth-type tls
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
  authentication eap-auth-type tls
```

**Related Commands**

```bash
no
```

Removes the RADIUS authentication settings
17.2.2 **chase-referral**

- **radius-server-policy**

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 disabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, 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><strong>no</strong></td>
<td>Disables LDAP server referral chasing</td>
</tr>
</tbody>
</table>
17.2.3 crl-check

Ensables 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 — AP300, 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, 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables CRL check on a RADIUS server policy</td>
</tr>
</tbody>
</table>
17.2.4 **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 — AP300, AP622, AP650, ES6510, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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</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>{on &lt;DEVICE-NAME&gt;}</td>
<td>Optional. Specifies the device name</td>
</tr>
<tr>
<td>&lt;DEVICE-NAME&gt;</td>
<td>Specify the name of the AP, wireless controller, or service platform.</td>
</tr>
<tr>
<td>Note:</td>
<td>To confirm the join status of a controller, use the <code>show &gt; ldap-agent &gt; join-status</code> command.</td>
</tr>
</tbody>
</table>

- `join-retry-timeout <60-300>`

| join-retry-timeout | If the join process fails (i.e. the RADIUS server fails to join the LDAP server’s domain), the process is retried after a specified interval. This command configures the interval (in seconds) between two successive join attempts. |
| <60-300> | Optional. 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>ldap-agent</th>
<th>Configures the LDAP agent’s settings</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
secondary | 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.

domain-name | This keyword is common to both the 'primary' and 'secondary' parameters.
<LDAP-DOMAIN-NAME> | - domain-name – Configures the primary or secondary LDAP server's domain name

| This keyword is common to both the 'primary' and 'secondary' parameters.

domain-admin-user | - domain-admin-user – Configures the primary or secondary LDAP server's admin user name
<ADMIN-USER-NAME> | - <ADMIN-USER-NAME> – Specify the admin user's name.

domain-admin-password | This keyword is common to both the 'primary' and 'secondary' parameters.
[0 <WORD>|2 <WORD>]] | - domain-admin-password – Configures the primary or secondary LDAP server’s admin user password
- 0 <WORD> – Specifies the password in the unencrypted format
- 2 <WORD> – Specifies the password in the encrypted format

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)#

rfs4000-229D58(config)#show session-config
!
Configuration of RFS4000 version 5.5.6.0-006D
!
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)#

Related Commands

no | Removes LDAP agent settings from this RADIUS server policy
17.2.5 ldap-group-verification

- radius-server-policy

Enables LDAP group verification settings on this RADIUS server policy.

Supported in the following platforms:
- Access Points — AP300, 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, 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>
17.2.6 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```yaml
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 <ATTR> group-attr <ATTR> group-filter <FILTER>
group-membership <WORD>
{net-timeout <1-10>}
```

Parameters

- `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.

- `ldap primary`
  - Configures the primary LDAP server settings

- `ldap secondary`
  - Configures the secondary LDAP server settings

- `host <IP>`
  - Specifies the LDAP host 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).
### 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)#
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#show context radius-server-policy test
testradius-policy-test
```

```bash
crl-check
```

```bash
dead-period 100
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#
```

```bash
rfs7000-37FABE(config-radius-server-policy-test)#
```

<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 DN names 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 <PASSWORD>|2 <ENCYPNTED-PASSWORD>|<PASSWORD>)] | Sets a valid password for the LDAP server.  
- 0 <PASSWORD> – Sets an UNENCRYPTED password  
- 2 <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. |
# Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables the LDAP server parameters</td>
</tr>
</tbody>
</table>
17.2.7 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX6500, NX6524, NX7500, 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>&lt;RADIUS-REALM&gt;</td>
<td>- 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
17.2.8 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

nas <IP/M> secret [0|2|<LINE>]

Changes the RADIUS client’s secret

Parameters

- nas <IP/M> secret [0 <LINE>|2 <LINE>]

<table>
<thead>
<tr>
<th>&lt;IP/M&gt;</th>
<th>Sets the RADIUS client’s IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• &lt;IP/M&gt; – Sets the RADIUS client’s IP address in the A.B.C.D/M format</td>
</tr>
</tbody>
</table>

| secret [0 <LINE>|2 <LINE>] | Sets the RADIUS client’s shared secret. Use one of the following options: |
|-----------------------------|------------------------------------------------|
| 0 <LINE> | • 0 <LINE> – Sets an UNENCRIPTED secret |
| 2 <LINE> | • 2 <LINE> – Sets an ENCRYPTED secret |
| <LINE> | • <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 163 login "test" bind-dn "bind-dn1" base-dn "base-dn1" passwd 0 test@123 passw-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
17.2.9 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [authentication|chase-referral|clr-check|ldap-agent|ldap-group-verification|ldap-server|local|nas|proxy|session-resumption|use]

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 use [radius-group [<RAD-GROUP-NAME>|all]|radius-user-pool-policy [<RAD-USER-POOL-NAME>|all]]

Parameters

- no authentication [data-source {ldap {fallback}|local}|eap configuration]

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-source</td>
<td>Removes the RADIUS authentication settings</td>
</tr>
<tr>
<td>ldap fallback</td>
<td>Optional. Removes a remote LDAP server as the data source for user authentication</td>
</tr>
<tr>
<td>ldap local</td>
<td>Optional. Enables fallback to local authentication in case LDAP authentication fails</td>
</tr>
<tr>
<td>ssid &lt;SSID&gt;</td>
<td>Optional. Removes the SSID associated with this LDAP data source</td>
</tr>
<tr>
<td>precedence &lt;1-5000&gt;</td>
<td>Specified the precedence from 1 -5000.</td>
</tr>
</tbody>
</table>

Note: Use this option to configure different data sources for each SSID.

eap configuration | Resets EAP authentication to the default mode |

- no [chase-referral|clr-check|ldap-group-verification|nas <IP/M>|session-resumption]

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no chase-referral</td>
<td>Disables LDAP server referral chasing</td>
</tr>
<tr>
<td>no crl-check</td>
<td>Removes the CRL check</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>no ldap-group-verification</code></td>
<td>Disables a RADIUS server’s LDAP group verification settings</td>
</tr>
</tbody>
</table>
| ```no nas``` | Removes a RADIUS server’s client  
  • `<IP/M>` – Sets the IP address of the RADIUS client in the A.B.C.D/M format |
| ```no session-resumption``` | Disables a RADIUS server’s session resumption settings |
| ```no ldap-agent [join-retry-timeout|primary|secondary]``` | Removes the LDAP agent parameters on this RADIUS server policy |
| ```join-retry-timeout``` | Removes the configured retry interval (this is the interval, in seconds, after which a access point or wireless controller retries joining the LDAP server’s domain) |
| ```primary``` | Removes the primary LDAP server details (such as, domain name, admin user name, and password) |
| ```secondary``` | Removes the secondary LDAP server details (such as, domain name, admin user name, and password) |
| ```no local realm [REALM-NAME]|all]``` | Removes a specified realm (specified by the `<REALM-NAME>` parameter) or all configured realms |
| ```no proxy [realm REALM-NAME]|retry-count|retry-delay]``` | Removes a RADIUS proxy server’s settings |
| ```realm REALM-NAME``` | Removes a proxy server’s realm name (specified by the `<REALM-NAME>` parameter) |
| ```retry-count``` | Removes a proxy server’s retry count |
| ```retry-delay``` | Removes a proxy server’s retry delay count |
| ```no ldap-server [dead-period|primary|secondary]``` | Disables the LDAP server parameters |
| ```dead-period``` | Sets the dead period as the duration the RADIUS server will not contact the LDAP server after finding it unavailable. |
| ```primary``` | Removes the primary LDAP server |
| ```secondary``` | Removes the secondary LDAP server |
| ```no use [radius-group [RAD-GROUP-NAME]|all]|radius-user-pool-policy [RAD-USER-POOL-NAME]|all]``` | Removes the RADIUS group or a RADIUS user pool policy |
| ```no use``` | Removes a RADIUS server’s local realm |
Examples
The following example shows the RADIUS server policy 'test' settings before the 'no' commands are executed:

```
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)#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:

```
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
```

Related Commands
- **radius-group <RAD-GROUP-NAME>**
  Removes a specified RADIUS group or all RADIUS groups
  - <RAD-GROUP-NAME> – Specify the RADIUS group name.
  - all – Removes all RADIUS groups

- **radius-user-pool-policy [<RAD-USER-POOL-NAME>][all]**
  Removes a specified RADIUS user pool or all RADIUS user pools
  - <RAD-USER-POOL-NAME> – Specify the RADIUS user pool name.
  - all – Removes all RADIUS user pools

- **authentication**
  Configures RADIUS server authentication parameters

- **chase-referral**
  Enables LDAP server referral chasing

- **crl-check**
  Enables a CRL check

- **ldap-agent**
  Configures the LDAP agent's parameters

- **ldap-group-verification**
  Enables LDAP group verification settings

- **ldap-server**
  Configures the LDAP server parameters. Configuring the LDAP server allows users to login and authenticate from anywhere on the network

- **local**
  Configures a local RADIUS realm on this RADIUS server policy

- **nas**
  Configures the key sent to a RADIUS client

- **proxy**
  Configures a proxy RADIUS server based on the realm/suffix
<table>
<thead>
<tr>
<th><strong>session-resumption</strong></th>
<th>Enables session resumption/fast re-authentication by using cached attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>use</strong></td>
<td>Defines settings used with the RADIUS server policy</td>
</tr>
</tbody>
</table>
### 17.2.10 proxy

> `radius-server-policy`

Configures 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** — AP300, 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, 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>]
  ```

  - **proxy realm** `<REALM-NAME>`
    - Configures the realm name
    - `<REALM-NAME>` – Specify the realm name. The name should not exceed 50 characters.

  - **server `<IP>`**
    - Configures the proxy server’s IP address. This is the address of server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server.
    - `<IP>` – Sets the proxy server’s IP address

  - **port `<1024-65535>`**
    - 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.
    - `<1024-65535>` – Sets the proxy server’s port from 1024 - 65535 (default port is 1812)

  - **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>`

retry-count <3-6>          Sets the proxy server’s retry count. This is the maximum number attempts made by a
                             controllers 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>`

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 is the 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 test123
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 test123
  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
17.2.11 session-resumption

Enables session resumption or fast re-authentication by using cached attributes. This feature controls the volume and duration of 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

\[
\text{session-resumption } \{\text{lifetime|max-entries}\}
\]

Parameters

- \(\text{session-assumption } \{\text{lifetime <1-24> \{max-entries <10-1024>\}}\|\text{max-entries <10-1024>}\}

| lifetime <1-24> \{max-entries <10-1024>\} | Optional. Sets the lifetime of cached entries
|---------------------------------------------|---------------------------------------------------------------------------------|
| \(\text{<1-24>}\) – Specify the lifetime period from 1 - 24 hours (default is 1 hour) | \(\text{max-entries} – \text{Optional. Configures the maximum number of entries in the cache}\)
| | \(\text{<10-1024>}\) – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries) |

- max-entries <10-1024> | Optional. Configures the maximum number of entries in the cache
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{&lt;10-1024&gt;}) – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)</td>
<td></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 172.16.10.7 port 1025 secret 0 test123
  ldap-server primary host 172.16.10.9 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 groupmembership2 net-timeout 2
  session-resumption lifetime 10 max-entries 11
rfs7000-37FABE(config-radius-server-policy-test)#

Related Commands

- \text{no} \quad \text{Disables session resumption on this RADIUS server policy}
17.2.12 use

radius-server-policy

Defines settings used with the RADIUS server policy

Supported in the following platforms:

- Access Points — AP300, 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, 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>]

- radius-group <RAD-GROUP-NAME1> \{RAD-GROUP-NAME2]\] 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.

- radius-user-pool-policy <RAD-USER-POOL-NAME> Associates a specified RADIUS user pool with this RADIUS server policy.
  Specify a user pool name.

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 test123
  ldap-server primary host 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
  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
17.3 radius-user-pool-policy

**RADIUS-POLICY**

Configures a RADIUS user pool policy

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)#
```

Table 17.3 summarizes RADIUS user pool policy configuration commands.

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>user</em></td>
<td>Configures the RADIUS user parameters</td>
<td>page 17-38</td>
</tr>
<tr>
<td><em>no</em></td>
<td>Negates a command or sets its default</td>
<td>page 17-38</td>
</tr>
</tbody>
</table>
17.3.1 user

radius-user-pool-policy

Configures RADIUS user parameters

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
user <USERNAME> password [0 <UNCRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
{group <RAD-GROUP> {<RAD-GROUP>|guest}}
user <USERNAME> password [0 <UNCRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
{group <RAD-GROUP> {guest expiry-time <HH:MM> expiry-date <MM:DD:YYYY>
{(email-id <EMAIL-ID>|start-time <HH:MM> start-date <MM:DD:YYYY>
 telephone <TELEPHONE-NUMBER>)}}}
```

Parameters

- `user <USERNAME>` — Adds a new RADIUS user to the RADIUS user pool
  - `<USERNAME>` — Specify the name of the user. The username should not exceed 64 characters.
  - **Note:** The username is a unique alphanumeric string identifying this user, and cannot be modified with the rest of the configuration.

- `passwd` Configures the user password (provide a password unique to this user)
  - 0 <UNENCRYPTED-PASSWORD> — Sets an unencrypted password
  - 2 <ENCRYPTED-PASSWORD> — Sets an encrypted password
  - <PASSWORD> — Sets a password (specified unencrypted) up to 21 characters

- `group <RAD-GROUP>` Optional. Configures the RADIUS server group of which this user is a member
  - `<RAD-GROUP>` — Specify a group name in the local database.
  - **Note:** If the user is a guest, assign the user a group with temporary access privileges.

- `guest` Optional. Specifies that this user is a guest user. Guest users have restricted access. After enabling a guest user account, specify the start and expiry time and date for this account.
  - A guest user can be assigned only to a guest user group.

- `expiry-time <HH:MM>` Optional. 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).

- `expiry-date <MM:DD:YYYY>` Optional. Specify the user account expiry date in the MM:DD:YYYY format (for example, 02:15:2014).

- `start-time <HH:MM>` Optional. Specify the user account activation time in the HH:MM format.

- `start-date <MM:DD:YYYY>` Optional. Specify the user account activation date in the MM:DD:YYYY format.
(email-id <EMAIL-ID> | start-time <HH:MM> | start-date <MM:DD:YYY> | telephone <TELEPHONE-NUMBER>)

| Examples |
|-----------------|---------------------------------|
| rfs7000-37FABE(config-radius-user-pool-testuser)#user testuser password 0 test@123 group test1 guest expiry-time 13:20 expiry-date 12:25:2014 start-time 17:00 start-date 01:05:2014 rfs7000-37FABE(config-radius-user-pool-testuser)#
| rfs7000-37FABE(config-radius-user-pool-testuser)#show context radius-user-pool-policy testuser user testuser password 0 test@123 group test1 guest expiry-time 13:20 expiry-date 12:25:2014 start-time 17:00 start-date 01:05:2014 rfs7000-37FABE(config-radius-user-pool-testuser)# |

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>* no *</td>
</tr>
</tbody>
</table>

After configuring the above user details, optionally configure the following user information:
- email-id – User's e-mail ID
- start-time – User's account activation time
- telephone – User’s telephone number (should include the area code)
17.3.2 no

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

no user <USERNAME>

Parameters

- no user <USERNAME>

<table>
<thead>
<tr>
<th>user &lt;USERNAME&gt;</th>
<th>Deletes a RADIUS user</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;USERNAME&gt;</td>
<td>Specify the user name.</td>
</tr>
</tbody>
</table>

Examples

The following example shows the RADIUS user pool ‘testuser’ settings before the ‘no’ command is executed:

```
rfs7000-37FABE(config-radius-user-pool-testuser)#show context
radius-user-pool-policy testuser
  user testuser password 0 test@123 group test1 guest expiry-time 13:20 expiry-date 12:25:2014 start-time 17:00 start-date 01:05:2014
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

```
rfs7000-37FABE(config-radius-user-pool-testuser)#no user testuser
```

The following example shows the RADIUS user pool ‘testuser’ settings after the ‘no’ command is executed:

```
rfs7000-37FABE(config-radius-user-pool-testuser)#show context
radius-user-pool-policy testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

Related Commands

- **user** | Configures the RADIUS user parameters |
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 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 than 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 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.

Controllers (access points, wireless 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.

Controllers 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: Statically 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.

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:

rfs7000-37FABE(config)#radio-qos-policy <POLICY-NAME>

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

rfs7000-37FABE(config-radio-qos-test)#
18.1 radio-qos-policy

Table 18.1 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 18-4</td>
</tr>
<tr>
<td>admission-control</td>
<td>Enables admission control across all radios for one or more access categories</td>
<td>page 18-5</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or resets configured settings to their default</td>
<td>page 18-8</td>
</tr>
<tr>
<td>smart-aggregation</td>
<td>Configures smart aggregation parameters</td>
<td>page 18-11</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands in the radio QoS configuration mode</td>
<td>page 18-13</td>
</tr>
<tr>
<td>wmm</td>
<td>Configures 802.11e/wireless multimedia parameters</td>
<td>page 18-15</td>
</tr>
</tbody>
</table>
### accelerated-multicast

Conifies multicast streams for acceleration. Multicasting allows group transmission of data streams.

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
accelerated-multicast [client-timeout | max-client-streams | max-streams | overflow-policy | stream-threshold]
```

```
accelerated-multicast [client-timeout <5-6000> | max-client-streams <1-4> | max-streams <0-256> | overflow-policy [reject | revert] | stream-threshold <1-500>]
```

#### Parameters

- **client-timeout**
  - `<5-6000>`
  - Configures a timeout period in seconds for wireless clients
  - `- <5-6000>` – Specify a value from 5 - 6000 seconds. The default is 60 seconds.

- **max-client-streams**
  - `<1-4>`
  - Configures the maximum number of accelerated multicast streams per client
  - `- <1-4>` – Specify a value from 1 - 4. The default is 2.

- **max-streams**
  - `<0-256>`
  - Configures the maximum number of accelerated multicast streams per radio
  - `- <0-256>` – Specify a value from 0 - 256. The default is 25.

- **overflow-policy**
  - `[reject | revert]`
  - Specifies the policy in case too many clients register simultaneously. The radio QOS policy can be configured to follow one of the following courses of action:
    - `reject` – Rejects new clients. The default overflow policy is reject.
    - `revert` – Reverts to regular multicast delivery

  **Note:** When the number of wireless clients using accelerated multicast exceeds the configured value (max-streams), the radio can either reject new wireless clients or revert existing clients to a non-accelerated state.

- **stream-threshold**
  - `<1-500>`
  - Configures the number of multicast packets per second threshold value. Once this threshold is crossed, the system triggers streams to accelerate.
  - `- <1-500>` – Specify a value from 1 - 500. The default is 25 packets per second.

#### 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
```

#### Related Commands

- **no**
  - Reverts accelerated multicasting settings to their default
### 18.1.2 admission-control

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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, 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-percent|
max-clients|max-roamed-clients|reserved-for-roam-percent}

admission-control [background|best-effort|video|voice] {max-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 TPSEC 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 TPSEC frames only. |

- **admission-control [background|best-effort|video|voice] {max-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>
<tbody>
<tr>
<td>max-percent &lt;0-150&gt;</td>
<td>Optional. Specifies the maximum percentage of airtime, including oversubscription, for the following access category:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</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;0-150&gt; – Specify a value from 0 - 150. This is the maximum percentage of airtime, including oversubscription, for the selected access category. The default is 75%.</td>
</tr>
<tr>
<td>max-clients &lt;0-256&gt;</td>
<td>Optional. Specifies the maximum number of wireless clients admitted to the following access categories:</td>
</tr>
<tr>
<td></td>
<td>• background – Sets the number of wireless clients supporting low (background) traffic allowed to exist (and consume bandwidth) within the radio’s QoS policy</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• video – Sets the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio’s QoS policy.</td>
</tr>
<tr>
<td></td>
<td>• voice – Sets the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio’s QoS policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</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;0-256&gt; – 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.</td>
</tr>
<tr>
<td>max-roamed-clients</td>
<td>Optional. Specifies the maximum number of roaming wireless clients admitted to the selected access category</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;0-256&gt;</td>
<td>- background – Sets the number of low (background) supported wireless clients allowed to roam to a different access point radio</td>
</tr>
<tr>
<td></td>
<td>- best-effort – Sets the number of normal (best-effort) supported wireless clients allowed to roam to a different access point radio</td>
</tr>
<tr>
<td></td>
<td>- video – Sets the number of video supported wireless clients allowed to roam to a different access point radio</td>
</tr>
<tr>
<td></td>
<td>- voice – Sets the number of voice supported wireless clients allowed to roam to a different access point radio</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;0-256&gt; – 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>reserved-for-roam-percent</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-150&gt;</td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</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;0-150&gt; – 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%.</td>
</tr>
</tbody>
</table>

**Examples**

```
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-percent 9
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
    admission-control voice max-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**

| no                   | Reverts or resets admission control settings to their default |
18.1.3 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

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]

no admission-control [firewall-detected-traffic|implicit-tspec]

no admission-control [background|best-effort|video|voice] {max-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 accelerated-multicast [client-timeout|max-client-streams|max-streams|overflow-policy|stream-threshold]

<table>
<thead>
<tr>
<th>no accelerated-multicast</th>
<th>Resets accelerated multicasting settings to their default. The following accelerated multicast control settings can be reverted:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• client-timeout – Resets the client timeout to the default (60 seconds)</td>
</tr>
<tr>
<td></td>
<td>• max-client-streams – Resets the maximum number of accelerated streams per client to default (2 streams per client)</td>
</tr>
<tr>
<td></td>
<td>• max-streams – Resets the maximum number of accelerated streams per radio to default (25 streams)</td>
</tr>
<tr>
<td></td>
<td>• overflow-policy – Resets the overflow policy to default (reject)</td>
</tr>
<tr>
<td></td>
<td>• stream-threshold – Resets the number of packets per second threshold to default (25 packets)</td>
</tr>
</tbody>
</table>

- no admission-control [firewall-detected-traffic|implicit-tspec]

<table>
<thead>
<tr>
<th>no admission-control</th>
<th>Reverts or resets admission control settings to their default. These controls are configured on a radio for one or more access categories.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• firewall-detected-traffic – Does not enforce admission control for traffic whose access category is detected by the firewall ALG</td>
</tr>
<tr>
<td></td>
<td>• implicit-tspec – Disables implicit traffic specifiers for wireless clients that do not support WMM-TSPEC</td>
</tr>
</tbody>
</table>
### no admission-control

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no admission-control</td>
<td>Reverts or resets admission control settings to their default. These controls are configured on a radio for one or more access categories.</td>
</tr>
<tr>
<td>background</td>
<td>Resets background access category admission control settings</td>
</tr>
<tr>
<td>best-effort</td>
<td>Resets best effort access category admission control settings</td>
</tr>
<tr>
<td>video</td>
<td>Resets video access category admission control settings</td>
</tr>
<tr>
<td>voice</td>
<td>Resets voice access category admission control settings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-percent</td>
<td>Resets the maximum percentage of airtime used by the selected access category to its default (75%)</td>
</tr>
<tr>
<td>max-clients</td>
<td>Resets the maximum number of wireless clients admitted by the selected access category to its default (100 clients)</td>
</tr>
<tr>
<td>max-roamed-clients</td>
<td>Resets the maximum number of roaming wireless clients admitted by the selected access category to its default (10 roaming clients)</td>
</tr>
<tr>
<td>reserved-for-roam-percent</td>
<td>Resets the percentage of air time allocated exclusively for roaming wireless clients by the selected access category to its default (10%)</td>
</tr>
</tbody>
</table>

### no smart-aggregation

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no smart-aggregation</td>
<td>Disable smart aggregation parameters</td>
</tr>
<tr>
<td>delay [background</td>
<td>best-effort</td>
</tr>
<tr>
<td>max-mesh-hops</td>
<td>Optional. Removes the configured maximum number of expected mesh hops</td>
</tr>
<tr>
<td>min-aggregation-limit</td>
<td>Optional. Removes the minimum number of aggregates buffered before an aggregate is sent</td>
</tr>
</tbody>
</table>

### no wmm

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no wmm</td>
<td>Reverts or resets 802.11e/wireless multimedia settings to default</td>
</tr>
<tr>
<td>background</td>
<td>Removes background access category wireless multimedia settings</td>
</tr>
<tr>
<td>best-effort</td>
<td>Removes best effort access category wireless multimedia settings</td>
</tr>
<tr>
<td>video</td>
<td>Removes video access category wireless multimedia settings</td>
</tr>
<tr>
<td>voice</td>
<td>Removes voice access category wireless multimedia settings</td>
</tr>
</tbody>
</table>

The following are common to the background, best-effort, video, and voice parameters:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aifsn</td>
<td>Removes the configured AIFSN value</td>
</tr>
<tr>
<td>cw-max</td>
<td>Removes the configured maximum contention window value</td>
</tr>
<tr>
<td>cw-min</td>
<td>Removes the configured minimum contention window value</td>
</tr>
<tr>
<td>txop-limit</td>
<td>Removes the configured transmit opportunity limit value</td>
</tr>
</tbody>
</table>
- no service admission-control across-reassoc

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no service admission-control across-reassoc</td>
<td>Disables retention of previously negotiated TSPEC parameters across re-associations on the radio</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the Radio-qos-policy 'test' settings before the 'no' commands are executed:

```
rfs7000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
  admission-control voice max-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-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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Configures multicast streams for acceleration. Multicasting allows the group transmission of data streams</td>
</tr>
<tr>
<td>admission-control</td>
<td>Enables admission control across all radios for one or more access categories</td>
</tr>
<tr>
<td>smart-aggregation</td>
<td>Configures smart aggregation parameters on this Radio QoS policy</td>
</tr>
<tr>
<td>service</td>
<td>Invokes service commands in the radio QoS configuration mode</td>
</tr>
<tr>
<td>wmm</td>
<td>Configures 802.11e wireless multimedia parameters</td>
</tr>
</tbody>
</table>
18.1.4 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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. • &lt;0-1000&gt; – Specify a value from 0 - 1000 msec.</td>
</tr>
</tbody>
</table>
**smart-aggregation** {max-mesh-hops <1-10>}

| max-mesh-hops <1-10> | Optional. Sets the maximum number of expected hops to the destination within a mesh  
| <1-10> – Specify a value from 1 - 10. The default is 3 hops. |

**smart-aggregation** {min-aggregation-limit <0-64>}

| min-aggregation-limit <0-64> | Optional. Sets the minimum number of aggregates buffered before an aggregate is sent  
| <0-64> – Specify a value from 0 - 64. The default is 8 frames. |

**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 |
18.1.5 service

Invokes service commands in the radio QoS configuration mode

Supported in the following platforms:
- Access Points — AP300, 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, 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)#

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)#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
          +--adoptee [show adoption log adoptee([on DEVICE-NAME])
          +--on
            +--DEVICE-NAME [show adoption log adoptee([on DEVICE-NAME])
          +--adaper [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

Note: For more information on admission-control parameters, see admission-control.
+DEVICE-NAME [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on DEVICE-NAME)]

--More--

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables retention of previously negotiated TSPEC parameters across re-associations on the radio</td>
</tr>
</tbody>
</table>
18.1.6 wmm

Configures 802.11e wireless multimedia (wmm) parameters

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```plaintext
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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wmm background</td>
<td>Configures background access category wireless multimedia settings</td>
</tr>
<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>
</tbody>
</table>
  - background – Sets the current AIFSN for low (background) traffic. The default is 7.
  - best-effort – Sets the current AIFSN for normal (best-effort) traffic. The default is 3.
  - 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.
  - 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.

The following keyword is common to all of the above traffic types:
- <1-15> – Sets a value from 1 - 15
**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.
- Recommends default WMM values be used 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.

---

**cw-max <0-15>**

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.

- **background** – Sets CW Max for low (background) traffic. The default is 10.
- **best-effort** – Sets CW Max for normal (best effort) traffic. The default is 6.
- **voice** – Sets CW Max for voice traffic. The default is 3.
- **video** – Sets CW Max for video traffic. The default is 4.

The following keyword is common to all of the above traffic types:

- **<0-15>** – ECW: the contention window. The actual value used is \((2^{ECW} - 1)\).

**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).

---

**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.

The following keyword is common to all of the above traffic types:

- **<0-15>** – ECW: the contention window. The actual value used is \((2^{ECW} - 1)\).

**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).

---

**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.

The following keyword is common to all of the above traffic types:

- **<0-65535>** – Specify a value from 0 - 65535 to configure the transmit opportunity limit in 32 microsecond units.

**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).
• TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

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-percent 9
  admission-control voice reserved-for-roam-percent 8
  accelerated-multicast stream-threshold 15
rfs7000-37FABE(config-radio-qos-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Reverts or resets 802.11e/wireless multimedia settings to their default</td>
</tr>
</tbody>
</table>
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
derend: 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-test)#
```
19.1 role-policy

Table 19.1 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 19-3</td>
</tr>
<tr>
<td>ldap-query</td>
<td>Enables LDAP service and specifies the LDAP server query mode</td>
<td>page 19-6</td>
</tr>
<tr>
<td>ldap-server</td>
<td>Configures the LDAP server settings</td>
<td>page 19-7</td>
</tr>
<tr>
<td>ldap-timeout</td>
<td>Configures the LDAP query timeout interval</td>
<td>page 19-9</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 19-10</td>
</tr>
<tr>
<td>user-role</td>
<td>Creates a role and associates it to the newly created role policy</td>
<td>page 19-12</td>
</tr>
</tbody>
</table>
### 19.1.1 default-role

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```markdown
default-role use [ip-access-list|mac-access-list]  

default-role use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>  
preference <1-100>
```

**Parameters**

- `default-role use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>` - Enables default role configuration. This role is applied to a wireless client not matching any of the user-defined roles.
  - Use — Associates an IP or a MAC access list with the default role
  - `[ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>` - Associates an IP access list or a MAC access list with this default role
    - `in` — Applies the rule (IP or MAC) to incoming packets
    - `out` — Applies the rule (IP 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/MAC-ACCESS-LIST-NAME>` — Specify the IP/MAC access list name.

**Note:** The IP and MAC ACL determine the action applied to a client assigned the default role.

**Precedence**

The following keyword is common to the IP and MAC access list parameters:

- `precedence <1-100>` — Specifies a precedence from 1 - 100.

**Note:** 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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes or resets the default role configuration</td>
</tr>
</tbody>
</table>
19.1.2 ldap-deadperiod

role-policy

Configures the Lightweight Directory Access Protocol (LDAP) deadperiod interval

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
ldap-deadperiod <60-300>

Parameters
- ldap-deadperiod <60-300>

| ldap-deadperiod <60-300> | 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.
| <60-300> | Specify the interval from 60 - 600 seconds. The default is 120 seconds.

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
### 19.1.3 `ldap-query`

- **role-policy**

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** — AP300, 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, 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 <code>ldap-server</code> 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.</td>
</tr>
</tbody>
</table>

**Note:** Use this option when the AP is layer 2 adopted to the controller.

**Examples**

```
rfs7000-37FABE(config-role-policy-test)#ldap-query self
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
rfs7000-37FABE(config-role-policy-test)#
```

**Related Commands**

- `no` Disables LDAP service on this role policy
### 19.1.4 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-server &lt;1-2&gt;</td>
<td>Specify the LDAP server ID from 1 - 2.</td>
</tr>
<tr>
<td>Note:</td>
<td>The primary LDAP server (ID 1) is used to bind and query. The secondary LDAP server (ID 2) is for failover.</td>
</tr>
<tr>
<td>host [&lt;IP&gt;</td>
<td>&lt;FQDN&gt;]</td>
</tr>
<tr>
<td>bind-dn &lt;BIND-DN&gt;</td>
<td>Specify the bind distinguished name (used for binding with the server).</td>
</tr>
<tr>
<td>base-dn &lt;BASE-DN&gt;</td>
<td>Specify the base distinguished name (used for searching). This should not exceed 127 characters.</td>
</tr>
<tr>
<td>bind-password &lt;PASSWORD&gt;</td>
<td>Specify the LDAP server password associated with the bind DN.</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Specify the LDAP server port from 1 - 65535. (default is 389).</td>
</tr>
<tr>
<td>server-type [active-directory</td>
<td>openldap]</td>
</tr>
</tbody>
</table>

**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-cn "CN=Administrator,CN=Users,DC=TechPub,DC=com" base-cn "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-cn "CN=Administrator,CN=Users,DC=TechPub,DC=com" base-cn "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
19.1.5 **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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

`ldap-timeout <1-5>`

**Parameters**

- `ldap-timeout <1-5>`

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ldap-timeout &lt;1-5&gt;</code></td>
<td>Configures the LDAP query timeout interval from 1 - 5 seconds (default is 2 seconds)</td>
</tr>
<tr>
<td></td>
<td>When enabled, LDAP service allows the AP or controller to bind with the LDAP server and query it for user details. The LDAP query timeout is the interval between a request to and the response from the LDAP server. Once this interval is exceeded, the LDAP bind and query is timed out.</td>
</tr>
</tbody>
</table>

**Examples**

rfs7000-37FABE(config-role-policy-test)#ldap-timeout 1

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=Adminstrator,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 query timeout to default (2 seconds)
### 19.1.6 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP81XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>
   precedence <1-100>
no user-role <ROLE-NAME>
```

**Parameters**
- `no [default-role|ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout]`
- `no ldap-deadperiod` Resets the LDAP dead period interval to default (120 seconds)
- `no ldap-query` Disables LDAP service on a role policy
- `no ldap-server <1-2>` Removes the selected LDAP server settings. Specify the LDAP server ID.
- `no ldap-timeout` Resets the LDAP timeout to default (2 seconds)
- `no default-role use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME> precedence <1-100>`
- `no user-role <ROLE-NAME>`
  - `no default-role use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME> precedence <1-100>`
  - `no user-role <ROLE-NAME>`
Examples
The following example shows the role policy 'test' setting before the 'no' commands are executed:

```
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=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)#
```

```
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)#
```

```
rfs7000-37FABE(config-role-policy-test)# show context
role-policy test
  default-role use ip-access-list in test precedence 1
  ldap-query self
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-role</td>
<td>Assigns a default role to a wireless client</td>
</tr>
<tr>
<td>ldap-deadperiod</td>
<td>Configures the LDAP deadperiod interval</td>
</tr>
<tr>
<td>ldap-query</td>
<td>Enables LDAP service on a role policy</td>
</tr>
<tr>
<td>ldap-server</td>
<td>Configures the LDAP server settings</td>
</tr>
<tr>
<td>ldap-timeout</td>
<td>Configures the LDAP server query timeout</td>
</tr>
<tr>
<td>user-role commands</td>
<td>Creates a role and associates it to the newly created role policy</td>
</tr>
</tbody>
</table>
19.1.7 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.

Table 19.2 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>19-13</td>
</tr>
<tr>
<td>user-role commands</td>
<td>Summarizes user role configuration mode commands</td>
<td>19-15</td>
</tr>
</tbody>
</table>
19.1.7.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
user-role <ROLE-NAME> precedence <1-10000>

Parameters
- user-role <ROLE-NAME> precedence <1-10000>

<table>
<thead>
<tr>
<th>user-role &lt;ROLE-NAME&gt;</th>
<th>Configures the user role name</th>
</tr>
</thead>
</table>
|                       | • <ROLE-NAME> Specify a name for this user role.

<table>
<thead>
<tr>
<th>precedence &lt;1-10000&gt;</th>
<th>Sets the precedence for this role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: Lower the precedence, higher is the role priority. Precedence determines the order in which a role is applied. If a wireless client matches multiple roles, the role with the lower precedence is applied before those with higher precedence. While there is no default precedence for a role, two or more roles can share the same precedence.</td>
<td></td>
</tr>
</tbody>
</table>

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
employeeid           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
ssid                 SSID configuration
state                State configuration
title                Title configuration
use                  Set setting to use
user-defined         User-defined 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

rfa7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

no                   Removes an existing user role
### 19.1.7.2 user-role commands

> **user-role**

Table 19.3 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 19-16</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 19-17</td>
</tr>
<tr>
<td>authentication-type</td>
<td>Configures an authentication type based filter</td>
<td>page 19-19</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures a captive portal based filter</td>
<td>page 19-21</td>
</tr>
<tr>
<td>city</td>
<td>Configures a city name based filter</td>
<td>page 19-22</td>
</tr>
<tr>
<td>client-identity</td>
<td>Associates a client-identity (device fingerprinting) based filter</td>
<td>page 19-23</td>
</tr>
<tr>
<td>company</td>
<td>Configures a company name based filter</td>
<td>page 19-24</td>
</tr>
<tr>
<td>country</td>
<td>Configures a country name based filter</td>
<td>page 19-25</td>
</tr>
<tr>
<td>department</td>
<td>Configures a department name based filter</td>
<td>page 19-26</td>
</tr>
<tr>
<td>emailid</td>
<td>Configures a e-mail ID based filter</td>
<td>page 19-28</td>
</tr>
<tr>
<td>employee-type</td>
<td>Configures a employee type ID based filter</td>
<td>page 19-30</td>
</tr>
<tr>
<td>employeeid</td>
<td>Configures a employee ID based filter</td>
<td>page 19-31</td>
</tr>
<tr>
<td>encryption-type</td>
<td>Configures an encryption type filter</td>
<td>page 19-33</td>
</tr>
<tr>
<td>group</td>
<td>Configures a RADIUS group based filter</td>
<td>page 19-35</td>
</tr>
<tr>
<td>memberOf</td>
<td>Assigns an Active Directory (AD) group to this user-defined role</td>
<td>page 19-36</td>
</tr>
<tr>
<td>mu-mac</td>
<td>Configures MAC address and mask based filter</td>
<td>page 19-37</td>
</tr>
<tr>
<td>no</td>
<td>Removes or resets the filters configured on this user-defined role</td>
<td>page 19-38</td>
</tr>
<tr>
<td>ssid</td>
<td>Configures a SSID based filter</td>
<td>page 19-41</td>
</tr>
<tr>
<td>state</td>
<td>Configures a user role state to match</td>
<td>page 19-43</td>
</tr>
<tr>
<td>title</td>
<td>Configures a ‘title’ string to match</td>
<td>page 19-44</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 19-45</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 19-47</td>
</tr>
</tbody>
</table>
19.1.7.2.1 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 — AP300, 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, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

\[\text{ap-location \{any|contains|exact|not-contains\}}\]

\[\text{ap-location any}\]

\[\text{ap-location \{contains|exact|not-contains\} <WORD>}\]

**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.
    - <WORD> – Specify the location string to match.

  - **exact <WORD>**
    
    Applies role if the associating AP's location exactly matches the string specified in the role.
    - <WORD> – Specify the exact location string to match.

  - **not-contains <WORD>**
    
    Applies role if the associating AP's location does not contain the location string specified in the role.
    - <WORD> – Specify the location string not to match.

**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.
**19.1.7.2.2 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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>**
  - 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

```
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)#

rfs4000-229D58 (config-role-policy-test-user-role-test)# commit
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
  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 Company, Santa Clara, USA onto vlan 2.

Create a new role policy with name ‘company-policy’.

```
create
<DEVICE> (config)# role-policy company-policy
```

Specify the LDAP server used for this role policy.

```
<DEVICE> (config-role-policy-company-policy)# ldap-query self
<DEVICE> (config-role-policy-company-policy)# ldap-server 1 host 192.160.1.1 bind-dn
CN=Administrator,CN=Users,DC=companyCompany,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 Company port 389
<DEVICE> (config-role-policy-company-policy)# ldap-timeout 2
```

Create a user defined role.

```
<DEVICE> (config-role-policy-company-policy)# user-role SCEngineer precedence 100
```

Define the role by adding appropriate values and match operators.

```
<DEVICE> (config-role-policy-company-policy-user-role-SCEngineer)# city exact santa-clara
<DEVICE> (config-role-policy-company-policy-user-role-SCEngineer)# company exact company
<DEVICE> (config-role-policy-company-policy-user-role-SCEngineer)# country exact usa
<DEVICE> (config-role-policy-company-policy-user-role-SCEngineer)# title contains engineer
<DEVICE> (config-role-policy-company-policy-user-role-SCEngineer)# assign vlan-id 2
```

Apply role policy to an access point.

```
ap7131-99BFA8 (config-device-ap7131)# use role-policy company-policy
```

Related Commands

```
no
Removes the upstream and/or downstream rate limits applied to this user-defined role. Also removes the VLAN ID.
```
### 19.1.7.2.3 authentication-type

**user-role commands**

Configures the authentication type based filter for this user-defined role.

Supported in the following platforms:
- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
authentication-type [any|eq|neq]
```

```
authentication-type any
```

```
authentication-type [eq|neq] [eap|kerberos|mac-auth|none]
```

```
{ (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) }

| eq [eap|kerberos|mac-auth|none]       | The role is applied only when the authentication type matches (equals) one or more than one of the following types: |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| • 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.

| neq [eap|kerberos|mac-auth|none]     | The role is applied only when the authentication type does not match (not equals) any of the following types: |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| • 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

| no                   | Removes the authentication type filter configured for this user-defined role |
19.1.7.2.4 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 — AP300, 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, 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
19.1.7.2.5 city

Configures a wireless client filter based on the city name

Supported in the following platforms:
- Access Points — AP300, 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, 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>]

| city | 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. |
| any | No specific city associated with this user-defined role. This role can be applied to any wireless client from any city. |
| contains <WORD> | The role is applied only when the city name, returned by the RADIUS server, contains the string specified in the role. |
| exact | The role is applied only when the city name, returned by the RADIUS server, exactly matches the string specified in the role. |
| 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. |

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 |
19.1.7.2.6 client-identity

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

Parameters

- client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}

Usage Guidelines

When associating a single or multiple client identities with a role policy, ensure that a client identity group, containing 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)#
r
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
19.1.7.2.7 company

**user-role commands**

Configures a wireless client filter based on the company name

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5524, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
company [any|contains|exact|not-contains]
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

**Parameters**

- `company [any|contains|exact|not-contains]`
  - 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 Company
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 Company
rfs7000-37FABE(config-role-policy-test-user-role-testing)#
```

**Related Commands**

- `no` Removes the company name configured with this user-defined role
19.1.7.2.8 country

user-role commands

Configures a wireless client filter based on the country name

Supported in the following platforms:
- Access Points — AP300, 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, 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>
</tbody>
</table>
| contains <WORD> | The role is applied only when the country 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 country name returned by the RADIUS server). It should contain the provided expression. |
| exact       | The role is applied only when the country 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 country name returned by the RADIUS server). It should be an exact match. |
| not-contains <WORD> | The role is applied only when the country 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 country name returned by the RADIUS server). It should not contain the provided expression. |

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 Company
  ...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
19.1.7.2.9 department

**user-role commands**

Configures a wireless client filter based on the department name

Supported in the following platforms:
- Access Points — AP300, 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, 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.  
- <WORD> – Specify the string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should contain the provided expression. |
| exact | The role is applied only when the department 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 department name returned by the RADIUS server). It should be an exact match. |
| 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.  
- <WORD> – Specify the string not to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should not contain the provided expression. |

**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 Company
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>
19.1.7.2.10 emailid

Configures a wireless client filter based on the e-mail ID

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
emailid [any|contains|exact|not-contains]
emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

Parameters
- emailid [any|exact <WORD>|contains <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@company.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 Company
country exact America
department exact TnV
  emailid exact testing@company.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><code>no</code></td>
<td>Removes the e-mail ID configured with this user-defined role</td>
</tr>
</tbody>
</table>
### 19.1.7.2.11 employee-type

#### user-role commands

Configures a wireless client filter based on the employee type

Supported in the following platforms:
- Access Points — AP300, 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, 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|contains|exact|not-contains]`: Specifies a wireless client filter based on how the 'employee type', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
- `employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`: Uses a specific employee type associated with this user-defined role.

<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>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The role is applied only when the employee type, 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 employee type 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 employee type, 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 employee type 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 employee type, 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 employee type returned by the RADIUS server). It should not contain the provided expression.</td>
</tr>
</tbody>
</table>

#### 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
### 19.1.7.2.12 employeed

**user-role commands**

Configures a wireless client filter based on the employee ID

Supported in the following platforms:

- **Access Points** — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
employeed [any|contains|exact|not-contains]
employeed [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

#### Parameters

- **employeed [any|contains <WORD>|exact <WORD>|not-contains <WORD>]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>employeed</strong></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><strong>any</strong></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><strong>contains &lt;WORD&gt;</strong></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></td>
<td>- &lt;WORD&gt; – 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><strong>exact</strong></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></td>
<td>- &lt;WORD&gt; – 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><strong>not-contains &lt;WORD&gt;</strong></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></td>
<td>- &lt;WORD&gt; – 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)#employeed contains TnVTest
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
department exact TnV
emailid exact testing@company.com
employeed contains TnVTest
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 employee ID configured with this user-defined role</td>
</tr>
</tbody>
</table>
### 19.1.7.2.13 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
encryption-type [any|eq|neq]
```

**encryption-type any**

```
encryption-type [eq|neq] [ccmp|keyguard|none|wep128|wep64]
{ (ccmp|keyguard|none|tkip-ccmp|wep128|wep64) }
```

**Parameters**

- **encryption-type any**
  
  | 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|wep128|wep64] { (ccmp|keyguard|none|tkip-ccmp|wep128|wep64) }**

**eq [ccmp|keyguard|none|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
- 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.

**neq [ccmp|keyguard|none|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
- 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 Company
  country exact America
  department exact TnV
  emailid exact testing@company.com
  employeeid contains TnVTest

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>
19.1.7.2.14 group

user-role commands

Configures a wireless client filter based on the RADIUS group name

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
group [any|contains|exact|not-contains]
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

- `group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group</code></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><code>any</code></td>
<td>This user-defined role can fit into any group (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 RADIUS group name contains the string specified in the role. <code>&lt;WORD&gt;</code> – Specify the string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should contain the provided expression.</td>
</tr>
<tr>
<td><code>exact &lt;WORD&gt;</code></td>
<td>The role is applied only when the RADIUS group name exactly matches the string specified in the role. <code>&lt;WORD&gt;</code> – Specify the exact string to match (this is case sensitive, and is compared against the group name 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 RADIUS group name does not contain the string specified in the role. <code>&lt;WORD&gt;</code> – Specify the string not to match (this is case sensitive, and is compared against the group 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)#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 Company
  country exact America
  department exact TnV
  emailid exact testing@company.com
  employeoid contains TnVTest
```

Related Commands

```
no
```

Removes the group configured for this user-defined role
### 19.1.7.2.15 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
memberOf <AD-GROUP-NAME>
```

**Parameters**

- `memberOf <AD-GROUP-NAME>`

**Examples**

```bash
rfs4000-229D58 (config-role-policy-test-user-role-test)#memberOf ADTestgroup
rfs4000-229D58 (config-role-policy-test-user-role-test)#
```

```bash
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
19.1.7.2.16 mu-mac

This command configures a MAC address and mask based filter for this role policy.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
mu-mac [<MAC> | any]
mu-mac any
mu-mac <MAC> {mask <MAC>}

Parameters
- mu-mac any
- mu-mac <MAC> {mask <MAC>}

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
  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 company
  country exact America
  department exact TnV
  emaillid exact testing@company.com
  employeeid contains TnVTest
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands
- no
  Removes the MAC address and mask for this user-defined role
19.1.7.2.17 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 — AP300, 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, 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|ssid|state|title|use|user-defined]
```

```
no [ap-location|assign|authentication-type|city|client-identity|company|country|
    department|emailid|employee-type|employeeid|encryption-type|group|mu-mac|memberOf|
    ssid|state|title|use|user-defined]
```

```
no captive-portal authentication-state
```

```
no use [ip-access-list|mac-access-list] [in|out] <IP/MAC-ACCESS-LIST-NAME>
```

```
precedence <1-100>
```

```
no use bonjour-gw-discovery-policy
```

**Parameters**
- no [ap-location|assign|authentication-type|city|client-identity|company|country|
  department|emailid|employee-type|employeeid|encryption-type|group|mu-mac|memberOf|
  ssid|state|title|user-defined]

<table>
<thead>
<tr>
<th>no ap-location</th>
<th>Removes an AP's deployment location filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>no assign</td>
<td>Removes the upstream and/or downstream rate limits and the VLAN ID associated with this user-defined role</td>
</tr>
<tr>
<td>no authentication-type</td>
<td>Removes the authentication type filter</td>
</tr>
<tr>
<td>no city</td>
<td>Removes the configured city name filter</td>
</tr>
<tr>
<td>no client-identity</td>
<td>Removes the client identity fingerprints based filter</td>
</tr>
<tr>
<td>no company</td>
<td>Removes the configured company name filter</td>
</tr>
<tr>
<td>no country</td>
<td>Removes the configured country name filter</td>
</tr>
<tr>
<td>no department</td>
<td>Removes the configured department name filter</td>
</tr>
<tr>
<td>no emailid</td>
<td>Removes the configured e-mail ID filter</td>
</tr>
<tr>
<td>no employee-type</td>
<td>Removes the configured employee-type filter</td>
</tr>
<tr>
<td>no employeeid</td>
<td>Removes the configured employee ID filter</td>
</tr>
<tr>
<td>no encryption-type</td>
<td>Removes the encryption type filter</td>
</tr>
<tr>
<td>no group</td>
<td>Removes the RADIUS group name filter</td>
</tr>
<tr>
<td>no memberOf</td>
<td>Removes the AD group based filter</td>
</tr>
</tbody>
</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 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 wepl28
  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 company
  country exact America
department exact TnV
  emailid exact testing@company.com
  employeoid contains TnVTest
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
city exact SanJose
country exact America
department exact TnV
emailid exact testing@company.com
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-location</td>
<td>Configures an AP deployment location based filter</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>
</tr>
<tr>
<td>authentication-type</td>
<td>Configures the authentication type filter</td>
</tr>
<tr>
<td>captive-portal</td>
<td>Configures a captive portal based filter</td>
</tr>
<tr>
<td>city</td>
<td>Configures a city name based filter</td>
</tr>
<tr>
<td>client-identity</td>
<td>Associates a client-identity (device fingerprinting) based filter with this user-defined role</td>
</tr>
<tr>
<td>company</td>
<td>Configures a company name based filter</td>
</tr>
<tr>
<td>country</td>
<td>Configures a country name based filter</td>
</tr>
<tr>
<td>department</td>
<td>Configures a department name based filter</td>
</tr>
<tr>
<td>emailid</td>
<td>Configures an e-mail ID based filter</td>
</tr>
<tr>
<td>employee-type</td>
<td>Configures an employee type based filter</td>
</tr>
<tr>
<td>employeeid</td>
<td>Configures an employee ID based filter</td>
</tr>
<tr>
<td>encryption-type</td>
<td>Configures the encryption type filter</td>
</tr>
<tr>
<td>group</td>
<td>Configures a RADIUS group based filter</td>
</tr>
<tr>
<td>memberOf</td>
<td>Configures an AD group based filter</td>
</tr>
<tr>
<td>mu-mac</td>
<td>Configures a MAC address and mask based filter</td>
</tr>
<tr>
<td>ssid</td>
<td>Configures a SSID based filter</td>
</tr>
<tr>
<td>state</td>
<td>Configures a state name based filter</td>
</tr>
<tr>
<td>title</td>
<td>Configures a user title based filter</td>
</tr>
<tr>
<td>use</td>
<td>Associates an IP and/or MAC ACL with this user-defined role</td>
</tr>
<tr>
<td>user-defined</td>
<td>Configures a user-defined filter (an attribute defined in AD or OpenLDAP server)</td>
</tr>
</tbody>
</table>
19.1.7.2.18 ssid

**user-role commands**

Configures a SSID based filter

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
ssid [any|exact|contains|not-contains]
```

```
ssid any
```

```
ssid [exact|contains|not-contains] <WORD>
```

**Parameters**

- **ssid any**
  
  Specifies a wireless client filter based on how the SSID is specified in a WLAN.
  
  - any – The role is applied to any SSID location. This is the default setting.

- **ssid [exact|contains|not-contains] <WORD>**
  
  Specifies a wireless client filter based on how the SSID is specified in a WLAN. This options are: contains, exact, or not-contains

  - exact <WORD>
    
    The role is applied only when the SSID, returned by the RADIUS server, exactly matches 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.

  - 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
country exact America
department exact TnV
emailid exact testing@company.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>
19.1.7.2.19 state

user-role commands

Configures a user role state to match with this user-defined role

Supported in the following platforms:

- Access Points — AP300, 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, 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>]

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
country exact America
department exact TnV
emailid exact testing@company.com
state exact active
rfs7000-37FABE(config-role-policy-test-user-role-testing)#

Related Commands

no

Removes the ‘state’ filter string associated with a user role
19.1.7.2.20 title

*user-role commands*

Configures a ‘title’ string to match

Supported in the following platforms:
- Access Points — AP300, 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, 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>
</tbody>
</table>
| contains <WORD> | The user role is applied only when the title string, 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 title returned by the RADIUS server). It should contain the provided expression. |
| exact <WORD> | The role is applied only when the title string, 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 title returned by the RADIUS server). It should be an exact match. |
| not-contains <WORD> | The role is applied only when the title string, 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 title returned by the RADIUS server). It should not contain the provided expression. |

**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
19.1.7.2.21 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

use [bonjour-gw-discovery-policy|ip-access-list|mac-access-list]

use bonjour-gw-discovery-policy <POLICY-NAME>

use ip-access-list [in|out] <IP-ACCESS-LIST-NAME> precedence <1-100>

use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>

**Parameters**

- **use bonjour-gw-discovery-policy <POLICY-NAME>**

  * **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 role.
    
    - **<POLICY-NAME>** – Specify the Bonjour GW Discovery policy name (should be existing and configured).
    
    **Note:** This feature is supported only on the RFS7000 and AP7131 devices.

    **Note:** For more information on Bonjour GW Discovery policy, see `bonjour-gw-discovery-policy`.

- **use ip-access-list [in|out] <IP-ACCESS-LIST-NAME> precedence <1-100>**

  * **ip-access-list [in|out]**
    
    Uses an IP access list with this user role.
    
    - **in** – Applies the rule to incoming packets
    - **out** – Applies the rule to outgoing packets

  * **<IP-ACCESS-LIST-NAME>**
    
    Specify the IP 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
### `use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`mac-access-list [in</td>
<td>out]`</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies the rule to incoming packets</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies the rule to outgoing packets</td>
</tr>
<tr>
<td><code>&lt;MAC-ACCESS-LIST-NAME&gt;</code></td>
<td>Specify the MAC access list name.</td>
</tr>
<tr>
<td><code>precedence &lt;1-100&gt;</code></td>
<td>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</td>
</tr>
<tr>
<td><code>&lt;1-100&gt;</code></td>
<td>Sets a precedence from 1 - 100</td>
</tr>
</tbody>
</table>

### Examples

```plaintext
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
eamarin exact testing@company.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-bonjour_test-user-role-bonjour_user1)#use bonjour-gw-discovery-policy role2
rfs7000-37FABE(config-role-policy-bonjour_test-user-role-bonjour_user1)#show context
user-role bonjour_user1 precedence 2
  use bonjour-gw-discovery-policy role2
rfs7000-37FABE(config-role-policy-bonjour_test-user-role-bonjour_user1)#

rfs7000-37FABE(config-role-policy-bonjour_test)#show context
role-policy bonjour_test
  user-role bonjour_user1 precedence 1
    mu-mac A4-D1-D2-BF-3D-19
    use bonjour-gw-discovery-policy role1
  user-role bonjour_user1 precedence 2
    mu-mac B0-65-BD-4B-BC-09
    use bonjour-gw-discovery-policy role2
rfs7000-37FABE(config-role-policy-bonjour_test)#
```

### 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>
19.1.7.2.22 user-defined

**user-defined 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
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>user-defined &lt;ATTR-STRING&gt;</th>
<th>Specify a filter based on an attribute defined in the AD or OpenLDAP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>No specific string to match. This role can be applied to any wireless client. This is the default setting.</td>
</tr>
<tr>
<td>contains &lt;WORD&gt;</td>
<td>The role is applied only when the user-defined attribute value, 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 user-defined attribute value, 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 user-defined attribute value, returned by the RADIUS server, does not contain the string specified in the role.</td>
</tr>
</tbody>
</table>

**Examples**

```
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**

- **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
- `channel-list` Select channel list for smart-rf
- `channel-width` Select channel width for smart-rf
- `coverage-hole-recovery` Recover from coverage hole
- `dfs` DFS related configuration
- `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 terminal

```
rfs7000-37FABE(config-smart-rf-policy-test)#
```
Table 20.1 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 20-4</td>
</tr>
<tr>
<td>assignable-power</td>
<td>Specifies the power range during power assignment</td>
<td>page 20-5</td>
</tr>
<tr>
<td>avoidance-time</td>
<td>Configures adaptivity timeout on channels</td>
<td>page 20-6</td>
</tr>
<tr>
<td>channel-list</td>
<td>Assigns the channel list for the selected frequency</td>
<td>page 20-7</td>
</tr>
<tr>
<td>channel-width</td>
<td>Selects the channel width for Smart RF configuration</td>
<td>page 20-8</td>
</tr>
<tr>
<td>coverage-hole-recovery</td>
<td>Enables recovery from errors</td>
<td>page 20-10</td>
</tr>
<tr>
<td>dfs</td>
<td>Allows a Smart RF enabled radio to avoid Dynamic Frequency Selection (DFS) regulated channels if radar is detected on those channels. This command also configures the period of avoidance.</td>
<td>page 20-12</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a Smart RF policy</td>
<td>page 20-13</td>
</tr>
<tr>
<td>group-by</td>
<td>Configures grouping parameters</td>
<td>page 20-14</td>
</tr>
<tr>
<td>interference-recovery</td>
<td>Recovers issues due to excessive noise and interference</td>
<td>page 20-15</td>
</tr>
<tr>
<td>neighbor-recovery</td>
<td>Enables recovery from errors due to faulty neighbor radios</td>
<td>page 20-17</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 20-19</td>
</tr>
<tr>
<td>sensitivity</td>
<td>Configures Smart RF sensitivity</td>
<td>page 20-21</td>
</tr>
<tr>
<td>smart-ocs-monitoring</td>
<td>Applies smart off channel scanning instead of dedicated detectors</td>
<td>page 20-22</td>
</tr>
</tbody>
</table>
20.1.1 area

 Configures the channel list and power for a specified area

 Supported in the following platforms:
 - Access Points — AP300, 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, 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)#

 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
### 20.1.2 assignable-power

**smart-rf-policy**

Specifies the power range during power assignment

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
assignable-power [2.4GHz|5GHz] [max|min] <1-20>
```

**Parameters**

- `assignable-power [2.4GHz|5GHz] [max|min] <1-20>`

| 2.4GHz [max|min] | Assigns a power range on the 2.4 GHz band |
|------------------|------------------------------------------|
| <1-20>           | - max <1-20> – Sets the upper limit in the range from 1 dBm - 20 dBm (default is 17 dBm) |
|                  | - min <1-20> – Sets the lower limit in the range from 1 dBm - 20 dBm (default is 4 dBm) |

| 5GHz [max|min] | Assigns a power range on the 5.0 GHz band |
|---------------|------------------------------------------|
| <1-20>        | - max <1-20> – Sets the upper limit in the range from 1 dBm - 20 dBm (default is 17 dBm) |
|               | - min <1-20> – Sets the lower limit in the range from 1 dBm - 20 dBm (default is 4 dBm) |

**Examples**

```
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
20.1.3 avoidance-time

- smart-rf-policy

Configures adaptivity timeout on channels. The channel is avoided till the adaptivity timeout expires.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

avoidance-time [adaptivity|dfs] <30-3600>

Parameters

- avoidance-time [adaptivity|dfs] <30-3600>

| avoidance-time [adaptivity|dfs] <30-3600> | Configures adaptivity timeout on channels. In case of ACS/SMART, the channel is avoided till adaptivity timeout expires. After that interval, the channel is free for use by both SMART and ACS. |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| • adaptivity <30-3600> | Configures adaptivity avoidance timeout. Specify a value from 30- 3600 minutes |
| • dfs <30-3600> | Configures dfs avoidance timeout. Specify a value from 30- 3600 minutes |

Examples

nx4500-5CFA2B(config-smart-rf-policy-p1)#avoidance-time dfs 30
nx4500-5CFA2B(config-smart-rf-policy-p1)#avoidance-time adaptivity 45
nx4500-5CFA2B(config-smart-rf-policy-p1)#
20.1.4 channel-list

Assigns a list of channels, for the selected frequency, used in Smart RF scans

Supported in the following platforms:
- Access Points — AP300, 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, 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
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
rfs7000-37FABE(config-smart-rf-policy-test)#

Related Commands

no
Removes the channel list for the selected frequency
20.1.5 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
channel-width [2.4GHz|5GHz]
channel-width 2.4GHz [20MHz|40MHz|auto]
channel-width 5GHz [20MHz|40MHz|80MHz|auto]
```

**Parameters**
- **channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]**

<table>
<thead>
<tr>
<th>Band</th>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz</td>
<td>[20MHz</td>
<td>40MHz</td>
</tr>
<tr>
<td></td>
<td>20MHz – Assigns the 20 MHz channel width. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>40MHz – Assigns the 40 MHz channel width</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auto – Assigns the best possible channel in the 20 MHz or 40 MHz channel width</td>
<td></td>
</tr>
<tr>
<td>5GHz</td>
<td>[20MHz</td>
<td>40MHz</td>
</tr>
<tr>
<td></td>
<td>20MHz – Assigns the 20 MHz channel width</td>
<td></td>
</tr>
<tr>
<td></td>
<td>40MHz – Assigns the 40 MHz channel width. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>80MHz – Assigns the 80 MHz channel width (supported only on AP8232)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auto – Assigns the best possible channel in the 20 MHz, 40 MHz, or 80 MHz channel width</td>
<td></td>
</tr>
</tbody>
</table>

**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 5 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

| no                      | Resets channel width for the selected frequency to its default |
20.1.6 coverage-hole-recovery

**smart-rf-policy**

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.

Supported in the following platforms:
- Access Points — AP300, 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, 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.
The following keywords are common to the ‘coverage-interval’ and ‘interval’ parameters:
- 5GHz <1-120> — Specifies a coverage hole recovery interval on the 5.0 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.

### 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
```
no
```
Disables recovery from coverage hole errors.
20.1.7 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. This command allows you 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
dfs avoidance-time <30-3600>
```

**Parameters**
- `dfs avoidance-time <30-3600>`

<table>
<thead>
<tr>
<th>dfs avoidance-time &lt;30-3600&gt;</th>
<th>Sets the time, in minutes, for which a radio avoids a DFS-regulated channel detected with a radar</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● <code>&lt;30-3600&gt;</code> – Specify a value from 30 - 3600 minutes. The default is 90 minutes.</td>
</tr>
</tbody>
</table>

**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)
20.1.8 **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** — AP300, 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, NX6524, NX7500, 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>
20.1.9 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 — AP300, 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, 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>

**Examples**

```plaintext
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
20.1.10 interference-recovery

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 radio'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.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

interference-recovery {channel-hold-time|channel-switch-delta|client-threshold|interference|neighbor-offset|noise|noise-factor}

Parameters

- interference-recovery {channel-switch-delta [2.4GHz|5GHZ] <5-35>}

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-switch-delta</td>
<td>Optional. Specifies the difference between the current and best channel interference needed to trigger a channel change. If the difference in noise levels on the current channel and a prospective channel is below the configured threshold, the channel is not changed.</td>
</tr>
<tr>
<td>[2.4GHz</td>
<td>5GHz]</td>
</tr>
<tr>
<td>&lt;5-35&gt;</td>
<td>Specifies the difference between the current and best channel interference</td>
</tr>
<tr>
<td></td>
<td>• &lt;5-35&gt; – Sets a value from 5 dBm - 35 dBm. The default setting is 20 dBm for both 2.4 GHz and 5.0 GHz bands.</td>
</tr>
</tbody>
</table>

- interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-hold-time</td>
<td>Optional. Defines the minimum time between two channel change recoveries</td>
</tr>
<tr>
<td>&lt;0-86400&gt;</td>
<td>• &lt;0-86400&gt; – Sets the time, in seconds, between channel change assignments based on interference or noise. The default is 7,200 seconds.</td>
</tr>
</tbody>
</table>

- client-threshold <1-255>  | Optional. Specifies client thresholds needed to avoid channel change. When the threshold number of clients are connected to a radio, the radio avoids changing channels even if the Smart RF master determines that a channel change is required. |
|                            | • <1-255> – Sets the number of clients from 1 - 255. The default is 50.                                                                       |
### Examples

```plaintext
rfs7000-37FABE(config-smart-rf-policy-test)#interference-recovery channel-switch-delta 5 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables recovery from excessive noise and interference</td>
</tr>
</tbody>
</table>
20.1.11 neighbor-recovery

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.

Supported in the following platforms:
- Access Points — AP300, 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, 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>}
  - dynamic-sampling Optional. Configures dynamic sampling on this Smart RF policy
  - retries <1-10> Optional. Specifies the number of retries before allowing a power level adjustments to compensate for a potential coverage hole.
    - <1-10> – Sets the number of retries from 1 - 10. The default is 3.
  - threshold <1-30> Optional. Specifies the minimum number of sample reports before which a power change requires dynamic sampling
    - <1-30> – Sets the minimum number of reports from 1 - 30. The default is 5.

- neighbor-recovery {power-hold-time <0-3600>}
  - power-hold-time Optional. Specifies the minimum time, in seconds, between two power changes on a radio during neighbor-recovery
  - <0-3600> Sets the time from 0 - 3600 sec. The default is 3600 seconds.

- neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}
  - power-threshold Optional. Specifies the power threshold based on the recovery performed
    - [2.4Ghz|5Ghz] Selects the band
      - 2.4GHz – Selects the 2.4 GHz band
      - 5GHz – Selects the 5.0 GHz band
**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
```

**Related Commands**

- `no` - Disables recovery from faulty neighbor radios
### 20.1.12 no

#### smart-rf-policy

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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
no [area|assignable-power|channel-list|channel-width|coverage-hole-recovery|dfs|
    enable|group-by|interference-recovery|neighbor-recovery|smart-ocs-monitoring]
```

#### Parameters

- `no area` Removes channel list/ power configuration for an area
- `no assignable-power` Resets assignable power to its default
- `no auto-assign-sensor` Disables auto assignment of sensor radios to its default
- `no channel-list` Resets the channel list for the selected frequency to its default
- `no channel-width` Resets channel width for the selected frequency to its default
- `no coverage-hole-recovery` Disables recovery from coverage hole errors
- `no dfs` Reverts the DFS-regulated channel avoidance time to default (90 minutes)
- `no enable` Disables a Smart RF policy
- `no group-by` Removes a Smart RF policy's group settings
- `no interference-recovery` Disables recovery from errors due to excessive noise and interference
- `no neighbor-recovery` Disables recovery from errors due to faulty neighbor radios
- `no smart-ocs-monitoring` Disables off channel monitoring

When used on an AP7161 model access point, this command disables a meshpoint.

#### Examples

The following example shows the Smart RF policy ‘test’ settings before 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
    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)#
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)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Specifies the channel list and power for a specified area</td>
</tr>
<tr>
<td>assignable-power</td>
<td>Assigns the power range</td>
</tr>
<tr>
<td>channel-list</td>
<td>Assigns the channel list for the selected frequency</td>
</tr>
<tr>
<td>channel-width</td>
<td>Selects the channel width for Smart RF configuration</td>
</tr>
<tr>
<td>coverage-hole-recovery</td>
<td>Enables recovery from coverage hole errors</td>
</tr>
<tr>
<td>dfs</td>
<td>Enables a Smart RF enabled radio to avoid Dynamic Frequency Selection (DFS) regulated channels if radar is detected on those channels. This command allows you to configure the period for which a radio avoids the DFS-regulated channel detected with a radar.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the configured Smart RF policy features</td>
</tr>
<tr>
<td>group-by</td>
<td>Configures grouping parameters on this Smart RF policy</td>
</tr>
<tr>
<td>interference-recovery</td>
<td>Enables recovery of errors due to excessive noise and interference</td>
</tr>
<tr>
<td>neighbor-recovery</td>
<td>Enables recovery of faulty neighbor radios</td>
</tr>
<tr>
<td>smart-ocs-monitoring</td>
<td>Applies smart off channel scanning instead of dedicated detectors</td>
</tr>
</tbody>
</table>
20.1.13 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 — AP300, 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, 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)#
### 20.1.14 `smart-ocs-monitoring`

**smart-rf-policy**

Applies smart *Off Channel Scanning* (OCS) instead of dedicated detectors

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```bash
smart-ocs-monitoring {awareness-override|client-aware|extended-scan-frequency|
  frequency|off-channel-duration|power-save-aware|sample-count|voice-aware}
smart-ocs-monitoring {awareness-override [schedule|threshold]}
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME> <DAY>}
smart-ocs-monitoring {awareness-override threshold <10-10000>}
smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}
smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}
smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}
smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}
smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}
smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
```

**Parameters**

- **smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME> <DAY>}

<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; &lt;END-TIME&gt; &lt;DAY&gt;</td>
<td>Configures a time and day schedule when awareness settings are overridden</td>
</tr>
<tr>
<td>&lt;1-3&gt; – Sets the awareness override schedule index. A maximum of three overrides can be configured.</td>
<td></td>
</tr>
<tr>
<td>&lt;START-TIME&gt; – Sets the override start time in HH:MM format</td>
<td></td>
</tr>
<tr>
<td>&lt;END-TIME&gt; – Sets the override end time in HH:MM format</td>
<td></td>
</tr>
<tr>
<td>DAY – Optional. Set the day when the override is active. Use one of the following formats:</td>
<td></td>
</tr>
</tbody>
</table>
  - 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>}

<table>
<thead>
<tr>
<th>awareness-override threshold &lt;10-10000&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Use this parameter to configure client awareness settings overrides</td>
</tr>
<tr>
<td>• threshold – Specifies the threshold after which client awareness settings are overridden. When the specified threshold is reached, awareness settings are overridden.</td>
</tr>
<tr>
<td>• &lt;10-10000&gt; – Specify a threshold value from 10 -10000. The default is 10.</td>
</tr>
</tbody>
</table>

### smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}

<table>
<thead>
<tr>
<th>client-aware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Enables client aware scanning on this Smart RF policy</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.4GHz &lt;1-255&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables client aware scanning on the 2.4 GHz band</td>
</tr>
<tr>
<td>Avoids radio scanning when a specified minimum number of clients are present</td>
</tr>
<tr>
<td>• &lt;1-255&gt; – Sets the minimum number of clients from 1 - 255. The default is 1 client.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5GHz &lt;1-255&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables client aware scanning on the 5.0 GHz band</td>
</tr>
<tr>
<td>Avoids radio scanning when a specified minimum number of clients are present</td>
</tr>
<tr>
<td>• &lt;1-255&gt; – Sets the minimum number of clients from 1 - 255. The default is 1 client.</td>
</tr>
</tbody>
</table>

### smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}

<table>
<thead>
<tr>
<th>extended-scan-frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.4GHz &lt;0-50&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables extended scan on the 2.4 GHz band</td>
</tr>
<tr>
<td>• &lt;0-50&gt; – Sets the number of trails from 0 - 50. The default is 5.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5GHz &lt;0-50&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables extended scan on the 5.0 GHz band</td>
</tr>
<tr>
<td>• &lt;0-50&gt; – Sets the number of trails from 0 - 50. The default is 5.</td>
</tr>
</tbody>
</table>

### smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}

<table>
<thead>
<tr>
<th>frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Specifies the scan frequency. This is the frequency, in seconds, in which smart-ocs-monitoring changes channels for an off channel scan.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.4GHz &lt;1-120&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects the 2.4 GHz band</td>
</tr>
<tr>
<td>• &lt;1-120&gt; – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5GHz &lt;1-120&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects the 5.0 GHz band</td>
</tr>
<tr>
<td>• &lt;1-120&gt; – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.</td>
</tr>
</tbody>
</table>

### smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}

<table>
<thead>
<tr>
<th>off-channel-duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional. Specifies the duration to scan off channel</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
### smart-ocs-monitoring

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smart-ocs-monitoring</td>
<td>`{power-save-aware [2.4GHz</td>
</tr>
<tr>
<td>power-save-aware</td>
<td>Optional. Enables power save awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict.</td>
</tr>
<tr>
<td>2.4GHz &lt;20-150&gt;</td>
<td>selects the 2.4 GHz band (in milliseconds)</td>
</tr>
<tr>
<td>5GHz &lt;20-150&gt;</td>
<td>selects the 5.0 GHz band (in milliseconds)</td>
</tr>
</tbody>
</table>
| 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  
  **Note:** The default is dynamic. |
| 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 (in milliseconds)                                                                                                   |
| 5GHz <1-15>      | selects the 5.0 GHz band (in milliseconds)                                                                                                   |
| voice-aware      | Optional. Enables voice awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict.                      |
| 2.4GHz [disable|dynamic|strict] | sets voice awareness 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] | sets voice awareness scanning mode on the 5.0 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. |
<table>
<thead>
<tr>
<th>Band</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz</td>
<td>Specifies the scanning mode on the 2.4 GHz band</td>
<td>[disable</td>
</tr>
<tr>
<td></td>
<td>disable – Disables voice awareness scanning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dynamic – Dynamically avoids scanning based on traffic for voice clients</td>
<td></td>
</tr>
<tr>
<td></td>
<td>strict – Strictly avoids scanning when voice clients are present</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The default is dynamic.</td>
<td></td>
</tr>
<tr>
<td>5GHz</td>
<td>Specifies the scanning mode on the 5.0 GHz band</td>
<td>[disable</td>
</tr>
<tr>
<td></td>
<td>dynamic – Dynamically avoids scanning based on traffic for voice clients</td>
<td></td>
</tr>
<tr>
<td></td>
<td>strict – Strictly avoids scanning when voice clients are present</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The default is dynamic.</td>
<td></td>
</tr>
</tbody>
</table>

**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>no</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 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:

```plaintext
<DEVICE>(config)#wips-policy <POLICY-NAME>

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

```plaintext
rfs7000-37FABE(config-wips-policy-test)#
```
### 21.1 wips-policy

Table 21.1 summarizes WIPS policy configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ap-detection</strong></td>
<td>Defines the WIPS AP detection configuration</td>
<td>page 21-4</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Enables a WIPS policy</td>
<td>page 21-5</td>
</tr>
<tr>
<td><strong>event</strong></td>
<td>Configures events</td>
<td>page 21-6</td>
</tr>
<tr>
<td><strong>history-throttle-duration</strong></td>
<td>Configures the duration event duplicates are omitted from the event history</td>
<td>page 21-10</td>
</tr>
<tr>
<td><strong>interference-event</strong></td>
<td>Specifies events contributing to the Smart RF WiFi interference calculations</td>
<td>page 21-11</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Negates a command or sets its default</td>
<td>page 21-12</td>
</tr>
<tr>
<td><strong>signature</strong></td>
<td>Configures a WIPS policy signature and enters its configuration mode</td>
<td>page 21-16</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>Defines a WIPS policy settings</td>
<td>page 21-34</td>
</tr>
</tbody>
</table>
## 21.1.1 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.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

### Syntax

```plaintext
ap-detection {ageout|wait-time}
ap-detection {age-out <30-86400>|wait-time <10-600>}
```

### Parameters

- `ap-detection {age-out <30-86400>|wait-time <10-600>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>age-out</td>
<td>Optional. Configures the unauthorized AP ageout interval. The WIPS policy uses this value to ageout unauthorized APs.</td>
</tr>
<tr>
<td>age-out &lt;30-86400&gt;</td>
<td>- Sets an ageout interval from 30 - 86400 seconds. The default is 5 minutes (300 seconds).</td>
</tr>
<tr>
<td>wait-time</td>
<td>Optional. Configures the wait time before a detected AP is declared as unauthorized and potentially removed</td>
</tr>
<tr>
<td>wait-time &lt;10-600&gt;</td>
<td>- Sets a wait time from 10 - 600 seconds. The default is 1 minute (60 seconds).</td>
</tr>
</tbody>
</table>

### Examples

```plaintext
rfs7000-37FABE(config-wips-policy-test)#ap-detection wait-time 15
rfs7000-37FABE(config-wips-policy-test)#ap-detection age-out 50
```

```plaintext
rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
  ap-detection-ageout 50
  ap-detection-wait-time 15
rfs7000-37FABE(config-wips-policy-test)#
```

### Related Commands

- `no` Resets unauthorized or unsanctioned AP detection settings to default
### 21.1.2 enable

- **wips-policy**

  Enables this WIPS policy

Supported in the following platforms:

- Access Points — AP300, 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, 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 | Disables a WIPS policy |
### 21.1.3 event

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.

Supported in the following platforms:
- **Access Points** — AP300, 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, 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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-anomaly</td>
<td>Enables AP anomaly event tracking. An AP anomaly event refers to suspicious frames sent by neighboring APs. An administrator enables or disables the filtering of each listed event and sets the thresholds for the generation of event notification and filtering.</td>
</tr>
<tr>
<td>ad-hoc-violation</td>
<td>Tracks ad-hoc network violations</td>
</tr>
<tr>
<td>airjack</td>
<td>Tracks AirJack attacks</td>
</tr>
<tr>
<td>ap-ssid-broadcast-in-beacon</td>
<td>Tracks AP SSID broadcasts in beacon events</td>
</tr>
<tr>
<td>asleap</td>
<td>Tracks ASLEAP attacks. These attacks break Lightweight Extensible Authentication Protocol (LEAP) passwords</td>
</tr>
<tr>
<td>impersonation-attack</td>
<td>Tracks impersonation attacks. These are also referred to as spoofing attacks, where the attacker assumes the address of an authorized device.</td>
</tr>
<tr>
<td>nullProbe-response</td>
<td>Tracks null probe response attacks</td>
</tr>
<tr>
<td>transmitting-device-using-invalid-mac</td>
<td>Tracks the transmitting device using an invalid MAC attacks</td>
</tr>
</tbody>
</table>
### WIPS-POLICY 21 - 7

<table>
<thead>
<tr>
<th><strong>unencrypted-wired-leakage</strong></th>
<th>Tracks unencrypted wired leakage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wireless-bridge</strong></td>
<td>Tracks wireless bridge (WDS) frames</td>
</tr>
</tbody>
</table>

- **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|wellenreiter] {filter-ageout <0-86400>}

  - **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) |

<table>
<thead>
<tr>
<th>excessive</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>80211-replay-check-failure</td>
<td>Tracks 802.11replay check failure</td>
</tr>
<tr>
<td>aggressive-scanning</td>
<td>Tracks aggressive scanning events</td>
</tr>
<tr>
<td>auth-server-failures</td>
<td>Tracks failures reported by authentication servers</td>
</tr>
<tr>
<td>decryption-failures</td>
<td>Tracks decryption failures</td>
</tr>
<tr>
<td>dos-assoc-or-auth-flood</td>
<td>Tracks DoS association or authentication floods</td>
</tr>
<tr>
<td>dos-eapol-start-storm</td>
<td>Tracks DoS EAPOL start storms</td>
</tr>
<tr>
<td>dos-unicast-deauth-or-disassoc</td>
<td>Tracks DoS dissociation or deauthentication floods</td>
</tr>
<tr>
<td>eap-flood</td>
<td>Tracks EAP floods</td>
</tr>
<tr>
<td>eap-nak-flood</td>
<td>Tracks EAP NAK floods</td>
</tr>
<tr>
<td>frames-from-unassoc-station</td>
<td>Tracks frames from unassociated clients</td>
</tr>
<tr>
<td>filter-ageout &lt;0-86400&gt;</td>
<td>The following keywords are common to all excessive events:</td>
</tr>
<tr>
<td></td>
<td>• filter-ageout &lt;0-86400&gt; – 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.</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-86400&gt; – Sets a filter ageout interval from 0 - 86400 seconds. The default is 0 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>threshold-client &lt;0-65535&gt;</td>
<td>The following keywords are common to all excessive events:</td>
</tr>
<tr>
<td></td>
<td>• threshold-client &lt;0-65535&gt; – Optional. Configures a client threshold value after which the filter is triggered and an event is recorded</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-65535&gt; – Sets a wireless client threshold value from 0 - 65535 seconds</td>
</tr>
<tr>
<td>threshold-radio &lt;0-65535&gt;</td>
<td>The following keywords are common to all excessive events:</td>
</tr>
<tr>
<td></td>
<td>• threshold-radio &lt;0-65535&gt; – Optional. Configures a radio threshold value after which the filter is triggered and an event is recorded</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-65535&gt; – Sets a radio threshold value from 0 - 65535 seconds</td>
</tr>
</tbody>
</table>
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

no | Disables WIPS policy events tracking
21.1.4 history-throttle-duration

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
history-throttle-duration <30-86400>
```

Parameters

- `history-throttle-duration <30-86400>`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history-throttle-duration &lt;30-86400&gt;</td>
<td>Configures the duration event duplicates are omitted from the event history</td>
</tr>
<tr>
<td></td>
<td>&lt;30-86400&gt; – Sets a value from 30 - 86400 seconds. The default is 120 seconds.</td>
</tr>
</tbody>
</table>

Examples

```
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

```
no
```

Resets the history throttle duration to its default (120 seconds)
21.1.5 interference-event

Specifies events contributing to the Smart RF WiFi interference calculations

Supported in the following platforms:
- Access Points — AP300, 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, 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
21.1.6 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [ap-detection|enable|event|history-throttle-duration|interference-event|signature|use]

no [enable|history-throttle-duration]

no ap-detection {ageout|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 [enable|history-throttle-duration]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no enable</td>
<td>Disables a WIPS policy from use with a profile</td>
</tr>
<tr>
<td>no history-throttle-duration</td>
<td>Resets the history throttle duration to its default (120 seconds). This is the duration event duplicates are omitted from the event history.</td>
</tr>
<tr>
<td>no ap-detection {ageout</td>
<td>wait-time} {&lt;LINE-SINK&gt;}</td>
</tr>
<tr>
<td>ageout &lt;LINE-SINK&gt;</td>
<td>Optional. Resets a rogue device's ageout interval to its default (300 seconds)</td>
</tr>
<tr>
<td>wait-time &lt;LINE-SINK&gt;</td>
<td>Optional. Resets the wait time value to its default (60 seconds)</td>
</tr>
</tbody>
</table>
- **no 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]

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no event ap-anomaly</td>
<td>Disables WIPS policy event tracking</td>
</tr>
<tr>
<td>ap-anomaly</td>
<td>Disables AP anomaly event tracking</td>
</tr>
<tr>
<td>ad-hoc-violation</td>
<td>Disables ad-hoc network violation event tracking</td>
</tr>
<tr>
<td>airjack</td>
<td>Disables the tracking of AirJack attacks</td>
</tr>
<tr>
<td>ap-ssid-broadcast-in-beacon</td>
<td>Disables the tracking of AP SSID broadcasts in beacon events</td>
</tr>
<tr>
<td>asleap</td>
<td>Disables the tracking of ASLEEP attacks</td>
</tr>
<tr>
<td>impersonation-attack</td>
<td>Disables the tracking of impersonation attacks</td>
</tr>
<tr>
<td>null-probe-response</td>
<td>Disables the tracking of null probe response attacks</td>
</tr>
<tr>
<td>transmitting-device-using-invalid-mac</td>
<td>Disables the tracking of invalid device MAC addresses</td>
</tr>
<tr>
<td>unencrypted-wired-leakage</td>
<td>Disables the tracking of unencrypted wired leakage detection</td>
</tr>
<tr>
<td>wireless-bridge</td>
<td>Disables the tracking of wireless bridge frames</td>
</tr>
</tbody>
</table>

- **no 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|wellenreiter]

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no event client-anomaly</td>
<td>Disables WIPS policy event tracking</td>
</tr>
<tr>
<td>client-anomaly</td>
<td>Disables client anomaly event tracking</td>
</tr>
<tr>
<td>dos-broadcast-deauth</td>
<td>Disables DoS broadcast deauthentication event tracking</td>
</tr>
<tr>
<td>fuzzing-all-zero-macs</td>
<td>Disables Fuzzing tracking: All zero MAC addresses observed</td>
</tr>
<tr>
<td>fuzzing-invalid-frame-type</td>
<td>Disables Fuzzing tracking: Invalid frame type detected</td>
</tr>
<tr>
<td>fuzzing-invalid-mgmt-frames</td>
<td>Disables Fuzzing tracking: Invalid management frame</td>
</tr>
<tr>
<td>fuzzing-invalid-seq-num</td>
<td>Disables Fuzzing tracking: Invalid sequence number</td>
</tr>
<tr>
<td>identical-src-and-dest-addr</td>
<td>Disables the tracking of identical source and destination addresses</td>
</tr>
<tr>
<td>invalid-8021x-frames</td>
<td>Disables Fuzzing tracking: Invalid 802.1x frames</td>
</tr>
<tr>
<td>netstumbler-generic</td>
<td>Disables Netstumbler (v3.2.0, 3.2.3, 3.3.0) event tracking</td>
</tr>
<tr>
<td>non-conforming-data</td>
<td>Disables non conforming data packet tracking</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>wellenreiter</td>
<td>Disables Wellenreiter event tracking</td>
</tr>
<tr>
<td>filter-ageout &lt;0-86400&gt;</td>
<td>The following keywords are common to all client anomaly events:</td>
</tr>
<tr>
<td></td>
<td>- Optional. Resets the filter expiration interval in seconds</td>
</tr>
<tr>
<td></td>
<td>- &lt;0-86400&gt; – Resets a filter ageout interval from 0 - 86400 seconds</td>
</tr>
<tr>
<td>no event</td>
<td>Disables WIPS policy event tracking</td>
</tr>
<tr>
<td>excessive</td>
<td>Disables the tracking of excessive events. Excessive events consist of actions that are performed</td>
</tr>
<tr>
<td></td>
<td>continuously and repetitively.</td>
</tr>
<tr>
<td>80211-replay-check-failure</td>
<td>Disables the tracking of 802.11 replay check failure</td>
</tr>
<tr>
<td>aggressive-scanning</td>
<td>Disables aggressive scanning event tracking</td>
</tr>
<tr>
<td>auth-server-failures</td>
<td>Disables the tracking of failures reported by authentication servers</td>
</tr>
<tr>
<td>decryption-failures</td>
<td>Disables the tracking of decryption failures</td>
</tr>
<tr>
<td>dos-assoc-or-auth-flood</td>
<td>Disables DoS association or authentication flood tracking</td>
</tr>
<tr>
<td>dos-eapol-start-storm</td>
<td>Disables the tracking of DoS EAPOL start storms</td>
</tr>
<tr>
<td>dos-unicast-deauth-or-disassoc</td>
<td>Disables DoS disassociation or deauthentication flood tracking</td>
</tr>
<tr>
<td>eap-flood</td>
<td>Disables the tracking of EAP floods</td>
</tr>
<tr>
<td>eap-nak-flood</td>
<td>Disables the tracking of EAP NAK floods</td>
</tr>
<tr>
<td>frames-from-unassoc-station</td>
<td>Disables the tracking of frames from unassociated clients</td>
</tr>
<tr>
<td>filter-ageout &lt;0-86400&gt;</td>
<td>Optional. Resets the filter expiration interval in seconds. It resets the duration for which a client</td>
</tr>
<tr>
<td></td>
<td>is filtered. The client is added to a ACL as a special entry and frames received from this client</td>
</tr>
<tr>
<td></td>
<td>are dropped.</td>
</tr>
<tr>
<td>- &lt;0-86400&gt; – Resets a filter ageout interval from 0 - 86400 seconds</td>
<td></td>
</tr>
<tr>
<td>threshold-client &lt;0-65535&gt;</td>
<td>Optional. Resets a client threshold limit after which the filter is triggered and an event is</td>
</tr>
<tr>
<td></td>
<td>recorded</td>
</tr>
<tr>
<td>- &lt;0-65535&gt; – Resets a wireless client threshold limit from 0 - 65535 seconds</td>
<td></td>
</tr>
<tr>
<td>threshold-radio &lt;0-65535&gt;</td>
<td>Optional. Resets a radio threshold limit after which an event is recorded</td>
</tr>
<tr>
<td></td>
<td>- &lt;0-65535&gt; – Resets a radio threshold limit from 0 - 65535 seconds</td>
</tr>
<tr>
<td>no interference-event</td>
<td>Disables interference event settings</td>
</tr>
<tr>
<td>non-conforming-data</td>
<td>Does not consider non conforming data packets when calculating Smart RF interference</td>
</tr>
<tr>
<td>wireless-bridge</td>
<td>Does not consider Wireless Bridge frames when calculating Smart RF interference</td>
</tr>
</tbody>
</table>
• no signature <WIPS-SIGNATURE>

<table>
<thead>
<tr>
<th>no signature</th>
<th>Deletes a WIPS policy signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;WIPS-SIGNATURE&gt;</td>
<td>Defines the unique name given to a WIPS policy signature</td>
</tr>
</tbody>
</table>

• no use device-categorization

| no use          | Disables the use of a device categorization policy with this WIPS policy |
| device-categorization | Resets the device categorization name to its default |

**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:

```
rrfs7000-37FABE(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
```

```
rrfs7000-37FABE(config-wips-policy-test)#no event client-anomaly wellenreiter
rrfs7000-37FABE(config-wips-policy-test)#no interference-event non-conforming-data
```

The following example shows the WIPS Policy ‘test’ settings after the ‘no’ commands are executed:

```
rrfs7000-37FABE(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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-detection</td>
<td>Enables the detection of unauthorized or unsanctioned access points</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a WIPS policy for use with a profile</td>
</tr>
<tr>
<td>event</td>
<td>Configures events, filters, and threshold values for a WIPS policy</td>
</tr>
<tr>
<td>history-throttle-duration</td>
<td>Configures the duration event duplicates are omitted from the event history</td>
</tr>
<tr>
<td>interference-event</td>
<td>Specifies events contributing to the Smart RF WiFi interference calculations</td>
</tr>
<tr>
<td>signature</td>
<td>Configures a WIPS policy signature</td>
</tr>
<tr>
<td>use</td>
<td>Enables the categorization of devices on this WIPS policy</td>
</tr>
</tbody>
</table>
21.1.7 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.

Table 21.2 summarizes WIPS policy signature configuration commands.

<table>
<thead>
<tr>
<th>signature</th>
<th>Configures a WIPS policy signature and enters its configuration mode</th>
<th>page 21-17</th>
</tr>
</thead>
<tbody>
<tr>
<td>signature mode commands</td>
<td>Summarizes WIPS signature configuration mode commands</td>
<td>page 21-19</td>
</tr>
</tbody>
</table>
21.1.7.1 signature

`signature`<br>

`signature <SIGNATURE-NAME>`<br>

**Configures a WIPS policy signature**<br>

**Supported in the following platforms:**<br>
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX<br>- Wireless Controllers — RFS4000, RFS6000, RFS7000<br>- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>
21.1.7.2 signature mode commands

Table 21.3 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 21-20</td>
</tr>
<tr>
<td>dst-mac</td>
<td>Configures the destination MAC address</td>
<td>page 21-21</td>
</tr>
<tr>
<td>filter-ageout</td>
<td>Configures the filter ageout interval</td>
<td>page 21-22</td>
</tr>
<tr>
<td>frame-type</td>
<td>Configures the frame type used for matching</td>
<td>page 21-23</td>
</tr>
<tr>
<td>interference-event</td>
<td>Configures this WIPS policy signature as the Smart RF interference source</td>
<td>page 21-25</td>
</tr>
<tr>
<td>mode</td>
<td>Enables or disables the signature mode</td>
<td>page 21-26</td>
</tr>
<tr>
<td>payload</td>
<td>Configures payload settings</td>
<td>page 21-27</td>
</tr>
<tr>
<td>src-mac</td>
<td>Configures the source MAC address</td>
<td>page 21-28</td>
</tr>
<tr>
<td>ssid-match</td>
<td>Configures a match based on SSID</td>
<td>page 21-29</td>
</tr>
<tr>
<td>threshold-client</td>
<td>Configures the wireless client threshold limit</td>
<td>page 21-30</td>
</tr>
<tr>
<td>threshold-radio</td>
<td>Configures the radio threshold limit</td>
<td>page 21-31</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 21-32</td>
</tr>
</tbody>
</table>
21.7.2.1 bssid

**signature mode commands**

Configures a BSSID MAC address with this WIPS signature for matching

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

bssid <MAC>

**Parameters**

- bssid <MAC>

<table>
<thead>
<tr>
<th>bssid &lt;MAC&gt;</th>
<th>Configures a BSSID MAC address to match</th>
</tr>
</thead>
</table>
| <MAC> – Specify the MAC address.

**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 BSS ID |
21.1.7.2.2 dst-mac

signature mode commands

Configures a destination MAC address for the packet examined for matching

Supported in the following platforms:

- Access Points — AP300, 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, 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 |
21.1.7.2.3 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

filter-ageout <1-86400>

**Parameters**

- filter-ageout <1-86400>

<table>
<thead>
<tr>
<th>filter-ageout &lt;1-86400&gt;</th>
<th>Configures the filter ageout interval from 1 - 86400 seconds</th>
</tr>
</thead>
</table>

**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
21.1.7.2.4 frame-type

**signature mode commands**

Configures the frame type used for matching with this WIPS policy signature.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>Configures the frame type used for matching</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**

```bash
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 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>Resets a WIPS signature frame type</td>
</tr>
</tbody>
</table>
21.1.7.2.5 interference-event

signature mode commands

Configures this WIPS policy signature as Smart RF interference source

Supported in the following platforms:

- Access Points — AP300, 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, 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

```
no
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables this WIPS policy signature as Smart RF interference source</td>
</tr>
</tbody>
</table>
21.1.7.2.6 mode

▶ signature mode commands

Enables or disables a WIPS policy signature

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

mode enable

Parameters

- mode enable

| mode enable | Enables this WIPS signature |

Examples

rfs7000-37FABE(config-test-signature-test)#mode enable
rfs7000-37FABE(config-test-signature-test)#

Related Commands

- no | Disables a WIPS signature |
21.1.7.2.7 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**
```
payload <1-3> pattern <WORD> offset <0-255>
```

**Parameters**
- **payload <1-3>** Configures payload settings
  - <1-3> — Sets the payload index
- **pattern <WORD>** Specifies the pattern to match: hex or string
  - <WORD> — Sets the pattern name
- **offset <0-255>** Specifies the payload offset to start the pattern match
  - <0-255> — Sets the offset value

**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)#
```

**Related Commands**
```
no
```
Removes payload and associated settings
21.1.7.2.8 src-mac

signature mode commands

Configures a source MAC address for a packet examined for matching

Supported in the following platforms:

- Access Points — AP300, 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, 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
21.1.7.2.9 ssid-match

- **signature mode commands**

Configures the SSID (and its character length) used for matching

Supported in the following platforms:
- Access Points — AP300, 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, 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>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssid &lt;SSID&gt;</code></td>
<td>Specifies the SSID match string</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;SSID&gt;</code> – Specify the SSID string.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Specify the correct SSID to ensure proper filtering.</td>
</tr>
<tr>
<td><code>ssid-len &lt;0-32&gt;</code></td>
<td>Specifies the length of the SSID</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;0-32&gt;</code> – Specify the SSID length from 0 - 32 characters.</td>
</tr>
</tbody>
</table>

**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
21.1.7.2.10 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
threshold-client <1-65535>
```

**Parameters**

- `threshold-client <1-65535>`

**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
```

**Related Commands**

```
o
```

Removes the wireless client threshold limit configured with a WIPS policy signature
21.1.7.2.11 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

threshold-radio <1-65535>

**Parameters**

- threshold-radio <1-65535>

<table>
<thead>
<tr>
<th>threshold-radio &lt;1-65535&gt;</th>
<th>Configures the radio’s threshold limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>• &lt;1-65535&gt; – Specify the threshold limit for a 60 second window from 1 - 65535.</td>
</tr>
</tbody>
</table>

**Examples**

```
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**

| no | Removes the radio’s threshold limit configured with a WIPS policy signature |
21.1.7.2.12 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 — AP300, 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, 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]
```

```
no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode enable|
    payload <1-3>|src-mac|ssid-match [ssid|ssid-len]|threshold-client|threshold-radio]
```

**Parameters**

- `no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode enable|
    payload <1-3>|src-mac|ssid-match [ssid|ssid-len]|threshold-client|threshold-radio]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no bssid</td>
<td>Disables a WIPS signature BSS ID</td>
</tr>
<tr>
<td>no dst-mac</td>
<td>Disables a WIPS signature destination MAC address</td>
</tr>
<tr>
<td>no filter-ageout</td>
<td>Removes the filter ageout interval. This is the duration a client, triggering a WIPS event, is excluded from RF Domain manager radio association.</td>
</tr>
<tr>
<td>no frame-type</td>
<td>Removes a WIPS signature frame type</td>
</tr>
<tr>
<td>no interference-event</td>
<td>Disables this WIPS policy signature as a Smart RF interference source</td>
</tr>
<tr>
<td>no mode enable</td>
<td>Disables a WIPS signature</td>
</tr>
<tr>
<td></td>
<td>• enable – Changes the mode from enabled to disabled</td>
</tr>
<tr>
<td>no payload &lt;1-3&gt;</td>
<td>Removes payload index and associated settings. The payload command sets a numerical index pattern and offset for this WIPS signature</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-3&gt; – Sets the payload index</td>
</tr>
<tr>
<td>no src-mac</td>
<td>Removes a WIPS signature source MAC address</td>
</tr>
<tr>
<td>no ssid-match [ssid</td>
<td>ssid-len]</td>
</tr>
<tr>
<td></td>
<td>• ssid – Removes the specified SSID match string</td>
</tr>
<tr>
<td></td>
<td>• ssid-len – Removes the specified character length of the SSID</td>
</tr>
<tr>
<td>no threshold-client</td>
<td>Removes the wireless client threshold limit configured with a WIPS policy. When the wireless client exceeds the specified limit, an event is triggered.</td>
</tr>
<tr>
<td>no threshold-radio</td>
<td>Removes a radio threshold limit configured with a WIPS policy. When the radio exceeds the specified threshold limit, an event is triggered.</td>
</tr>
</tbody>
</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 is the WIPS signature ‘test’ settings before the execution of the ‘no’ command:

```bash
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:

```bash
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)
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bssid</strong></td>
<td>Configures a WIPS signature BSSID MAC address</td>
</tr>
<tr>
<td><strong>dst-mac</strong></td>
<td>Configures a destination MAC address for the packet examined for matching</td>
</tr>
<tr>
<td><strong>filter-ageout</strong></td>
<td>Configures the filter ageout interval</td>
</tr>
<tr>
<td><strong>frame-type</strong></td>
<td>Configures the frame type to match with a signature</td>
</tr>
<tr>
<td><strong>interference-event</strong></td>
<td>Specifies events contributing to the Smart RF WiFi interference calculations</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>Enables or disables a WIPS signature</td>
</tr>
<tr>
<td><strong>payload</strong></td>
<td>Configures payload settings. The payload command sets a numerical index pattern and offset for this WIPS signature.</td>
</tr>
<tr>
<td><strong>src-mac</strong></td>
<td>Configures a source MAC address for the packet examined for matching</td>
</tr>
<tr>
<td><strong>ssid-match</strong></td>
<td>Configures a SSID for matching</td>
</tr>
<tr>
<td><strong>threshold-client</strong></td>
<td>Configures a wireless client threshold limit</td>
</tr>
<tr>
<td><strong>threshold-radio</strong></td>
<td>Configures a radio threshold limit</td>
</tr>
</tbody>
</table>
21.1.8 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 — AP300, 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, 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
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)#
22.1 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.

Table 22.1 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 22-3</td>
</tr>
<tr>
<td>classification</td>
<td>Classifies WLAN traffic based on priority</td>
<td>page 22-5</td>
</tr>
<tr>
<td>multicast-mask</td>
<td>Configures the egress prioritization multicast mask</td>
<td>page 22-7</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 22-8</td>
</tr>
<tr>
<td>qos</td>
<td>Defines the QoS configuration</td>
<td>page 22-11</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Configures the WLAN traffic rate limit using a WLAN QoS policy</td>
<td>page 22-12</td>
</tr>
<tr>
<td>svp-prioritization</td>
<td>Enables Spectralink voice protocol support on a WLAN</td>
<td>page 22-15</td>
</tr>
<tr>
<td>voice-prioritization</td>
<td>Prioritizes voice client over other clients</td>
<td>page 22-16</td>
</tr>
<tr>
<td>wmm</td>
<td>Configures 802.11e/wireless multimedia parameters</td>
<td>page 22-17</td>
</tr>
</tbody>
</table>
### 22.1.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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>accelerated-multicast</td>
<td>Configures the accelerated multicast stream address and forwarding QoS classification</td>
</tr>
<tr>
<td>&lt;IP&gt;</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>autodetect</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>classification</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>background</td>
<td>Forwards streams with background (low) priority. This parameter is common to both &lt;IP&gt; and autodetect.</td>
</tr>
<tr>
<td>best-effort</td>
<td>Forwards streams with best effort (normal) priority. This parameter is common to both &lt;IP&gt; and autodetect.</td>
</tr>
<tr>
<td>trust</td>
<td>No change to the streams forwarding traffic class. This parameter is common to both &lt;IP&gt; and autodetect.</td>
</tr>
<tr>
<td>video</td>
<td>Forwards streams with video traffic priority. This parameter is common to both &lt;IP&gt; and autodetect.</td>
</tr>
<tr>
<td>voice</td>
<td>Forwards streams with voice traffic priority. This parameter is common to both &lt;IP&gt; 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)#
```
### 22.1.2 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>classification [low</td>
</tr>
<tr>
<td>classification [low</td>
</tr>
<tr>
<td>classification non-unicast [voice</td>
</tr>
<tr>
<td>classification non-wmm [voice</td>
</tr>
</tbody>
</table>

**Parameters**

- `classification [low|normal|video|voice|wmm]`
- `classification non-unicast [voice|video|normal|low|default]`

<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.</td>
</tr>
<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>
classification non-wmm [voice|video|normal|low]

<table>
<thead>
<tr>
<th>low</th>
<th>Optimized for non-unicast background traffic. Implies all WLAN non-unicast traffic is classified and treated as low priority packets (background)</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the default classification mode (same as unicast classification if WMM is disabled, normal if unicast classification is WMM)</td>
</tr>
</tbody>
</table>

- classification non-wmm [voice|video|normal|low]

<table>
<thead>
<tr>
<th>non-wmm</th>
<th>Specifies how traffic from non-WMM clients is classified</th>
</tr>
</thead>
<tbody>
<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)</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

```
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
  qos trust dscp
  qos trust wmm
  accelerated-multicast autodetect
classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```
22.1.3 multicast-mask

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
multicast-mask [primary|secondary] <MAC/MASK>

Parameters
- multicast-mask [primary|secondary] <MAC/MASK>

| primary <MAC/MASK> | Configures the primary egress prioritization multicast mask
|                    | • <MAC/MASK> – Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF/XX-XX-XX-XX-XX-XX format
|                    | **Note:** Setting masks is optional and only needed if there are traffic types requiring special handling.

| secondary <MAC/MASK> | Configures the primary egress prioritization multicast mask
|                     | • <MAC/MASK> – Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF / XX-XX-XX-XX-XX-XX format

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
go trust dscp
go trust wmm
accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
### 22.1.4 no

Negates a command or resets settings to their default

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no rate-limit [client</td>
<td>wlan] [from-air</td>
</tr>
<tr>
<td>no wmm [background</td>
<td>best-effort</td>
</tr>
</tbody>
</table>

**Parameters**

- no <IP> – Removes specified IP address. Specify the IP address |
- no autodetect – Disables multicast streams automatic detection |
- no non-unicast – Optional. Removes multicast and broadcast packet classification |
- no non-wmm – Optional. Removes non-WMM client traffic classification |
- no primary – Removes the first egress multicast mask |
- no secondary – Removes the second egress multicast mask |
- no trust – Ignores the trust QoS values of ingressing packets |
- no dscp – Ignores the IP DSCP values of ingressing packets |
- no wmm – Ignores the 802.11 WMM QoS values of ingressing packets |
- no SVP support on a WLAN |
- no voice client priority over other clients (applies to non-WMM clients) |
**WLAN-QoS-Policy 22 - 9**

- `no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold [background|best-effort|video|voice]}`

| no rate-limit [client|wlan] | Disables traffic rate limit parameters  
|                            | • Disables client traffic rate limits  
|                            | • Disables WLAN traffic rate limits  
| [from-air|to-air]           | The following are common to the client and WLAN parameters:  
|                            | • from-air – Removes client/WLAN traffic rate limits in the up link direction. This is traffic from the wireless client to the network  
|                            | • to-air – Removes client/WLAN traffic rate limits in the down link direction. This is traffic from the network to the wireless client  
| max-burst-size             | Optional. Disables the maximum burst size value  
| rate                      | Optional. Disables the traffic rates configured for a wireless client or WLAN  
| red-threshold              | Optional. Disables random early detection threshold values configured for the traffic class  
|                            | • background – Disables the low priority traffic (background) threshold value  
|                            | • best-effort – Disables the normal priority traffic (best effort) threshold value  
|                            | • video – Disables the video traffic threshold value  
|                            | • voice – Disables the voice traffic threshold value  

- `no wmm [power-save|qbss-load-element]`

| no wmm                         | Disables 802.11e/wireless multimedia parameters  
| power-save                     | Disables support for WMM-Powersave (U-APSD)  
| qbss-load-element              | Disables support for the QBSS load information element in beacons and probe responses  

- `no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]`

| no wmm                         | Disables 802.11e/wireless multimedia parameters  
| background                     | Disables background access category parameters  
| best-effort                    | Disables best effort access category parameters  
| video                          | Disables video access category parameters  
| voice                          | Disables voice access category parameters  

**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 11-22-33-44-55-66-77  
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)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Configures the accelerated multicast streams address and forwards the QoS classification</td>
</tr>
<tr>
<td>classification</td>
<td>Classifies WLAN traffic based on priority</td>
</tr>
<tr>
<td>multicast-mask</td>
<td>Configures the egress prioritization multicast mask</td>
</tr>
<tr>
<td>qos</td>
<td>Defines the QoS configuration</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Configures a WLAN's traffic rate limits</td>
</tr>
<tr>
<td>svp-prioritization</td>
<td>Enables Spectralink voice protocol support on a WLAN</td>
</tr>
<tr>
<td>voice-prioritization</td>
<td>Prioritizes voice client over other clients</td>
</tr>
<tr>
<td>wmm</td>
<td>Configures the 802.11e/wireless multimedia parameters</td>
</tr>
</tbody>
</table>
22.1.5 qos

* wlan-qos-policy

Enables QoS on this WLAN

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
gos trust [dscp|wmm]
```

**Parameters**

- `trust [dscp|wmm]`

| trust [dscp|wmm] | Trusts the QoS values of ingressing packets |
|-----------------|-------------------------------------------|
| dscp            | Trusts the IP DSCP values of ingressing packets |
| wmm             | Trusts the 802.11 WMM QoS values of ingressing packets |

**Examples**

```plaintext
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)#
```
22.1.6 rate-limit

Configures 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 traffic).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, 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 — AP300, 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, 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>}
- max-burst-size <2-1024> 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 is 320 kbytes.
  
  **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>rate &lt;50-1000000&gt;</th>
<th>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 is 5000 kbps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit [client</td>
<td>wlan] [from-air</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>rate-limit</th>
<th>Configures traffic rate limit parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Configures traffic rate limiting parameters on a per-client basis</td>
</tr>
<tr>
<td>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>red-threshold</td>
<td>Configures random early detection threshold values for a designated traffic class</td>
</tr>
<tr>
<td>background &lt;0-100&gt;</td>
<td>The following is common to the ‘from-air’ and ‘to-air’ parameters: Optional. Sets a percentage value for background traffic in the upstream or downstream direction. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50% for traffic in both directions.</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 is 50% for traffic in both directions.</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 is 25% for traffic in both directions.</td>
</tr>
<tr>
<td>voice &lt;0-100&gt;</td>
<td>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 is 0% for traffic in both directions. 0% means no early random drops will occur.</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

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
rfs7000-37FABE(config-wlan-qos-test)#

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
gos trust wmm
accelerated-multicast autodetect classification voice

rfs7000-37FABE(config-wlan-qos-test)#
22.1.7 svp-prioritization

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 enabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
svp-prioritization

Parameters
None

Examples
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)#
22.1.8 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 enabled by default.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
voice-prioritization

Parameters
None

Examples
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
voice-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)#
### 22.1.9 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 — AP300, 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, 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]` Configures 802.11e/wireless multimedia parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wmm</td>
<td>Enables support for the WMM-Powersave mechanism. This mechanism, also known as UAPS-D, is specifically designed for WMM voice devices.</td>
</tr>
<tr>
<td>power-save</td>
<td>Enables support for the QoS Basic Service Set (QBSS) load information element in beacons and probe response packets advertised by access packets. This feature is enabled by default.</td>
</tr>
</tbody>
</table>
- **wmm** [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]

<table>
<thead>
<tr>
<th><strong>wmm</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>background</strong></td>
<td>Configures background access category parameters</td>
</tr>
<tr>
<td><strong>best-effort</strong></td>
<td>Configures best effort access category parameters. Packets not assigned to any particular access category are categorized by default as having best effort priority</td>
</tr>
<tr>
<td><strong>video</strong></td>
<td>Configures video access category parameters</td>
</tr>
<tr>
<td><strong>voice</strong></td>
<td>Configures voice access category parameters</td>
</tr>
<tr>
<td><strong>aifsn &lt;2-15&gt;</strong></td>
<td>Configures <em>Arbitrary Inter-Frame Space Number</em> (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 • &lt;2-15&gt; – Sets a value from 2 - 15</td>
</tr>
<tr>
<td><strong>cw-max &lt;0-15&gt;</strong></td>
<td>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 is 10 The default for traffic background (low) categories is 10 • &lt;0-15&gt; – ECW: the contention window. The actual value used is (2^{\text{ECW}} - 1). Set a value from 0 - 15.</td>
</tr>
<tr>
<td><strong>cw-min &lt;0-15&gt;</strong></td>
<td>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 • &lt;0-15&gt; – ECW: the contention window. The actual value used is (2^{\text{ECW}} - 1). Set a value from 0 - 15.</td>
</tr>
</tbody>
</table>
### Examples

```
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
```

- **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.
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 (a 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`
23.1 l2tpv3-policy-commands

Use the (config) instance to configure L2TPv3 policy parameters. To navigate to the L2TPv3 policy instance, use the following commands:

```bash
<DEVICE>(config)#l2tpv3 policy <L2TPV3-POLICY-NAME>
```

```bash
rfs7000-37FABE(config)#l2tpv3 policy L2TPV3Policy1
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

```bash
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-12-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 acknowledgment.
- **tx-window-size**: Number of signaling messages that can be sent without receiving the acknowledgment.
- **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-l2tpv3-policy-L2TPV3Policy1)#
```

Table 23.1 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 23-5</td>
</tr>
<tr>
<td>failover-delay</td>
<td>Configures the L2TPv3 tunnel failover delay in seconds</td>
<td>page 23-6</td>
</tr>
<tr>
<td>force-12-path-recovery</td>
<td>Enables the forced detection of servers and gateways behind the L2TPv3 tunnel</td>
<td>page 23-7</td>
</tr>
</tbody>
</table>
### Table 23.1 L2TPv3-Tunnel-Policy-Config Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hello-interval</code></td>
<td>Configures the interval, in seconds, between L2TPv3 “Hello” keep-alive messages exchanged in the L2TPv3 control connection</td>
<td>page 23-8</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negates or reverts L2TPv3 tunnel commands</td>
<td>page 23-9</td>
</tr>
<tr>
<td><code>reconnect-attempts</code></td>
<td>Configures the maximum number of retransmissions for signalling messages</td>
<td>page 23-11</td>
</tr>
<tr>
<td><code>reconnect-interval</code></td>
<td>Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection</td>
<td>page 23-12</td>
</tr>
<tr>
<td><code>retry-attempts</code></td>
<td>Configures the maximum number of retransmissions of signalling messages</td>
<td>page 23-13</td>
</tr>
<tr>
<td><code>retry-interval</code></td>
<td>Configures the interval, in seconds, before initiating a retransmission of any L2TPv3 signalling message</td>
<td>page 23-14</td>
</tr>
<tr>
<td><code>rx-window-size</code></td>
<td>Configures the number of signalling messages received without sending an acknowledgment</td>
<td>page 23-15</td>
</tr>
<tr>
<td><code>tx-window-size</code></td>
<td>Configures the number of signalling messages transmitted without receiving an acknowledgment</td>
<td>page 23-16</td>
</tr>
</tbody>
</table>
23.1.1 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
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: |
|---------------------|------------------------------------------------------------------------------------------|
| 0                   | 0 – No cookie field present in each L2TPv3 data message (this is the default setting)     |
| 4                   | 4 – 4 byte cookie field present in each L2TPv3 data message                              |
| 8                   | 8 – 8 byte cookie field present in each L2TPv3 data message                              |

**Examples**

```
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**

- `no`
  
  Resets the cookie-field size to its default (0 - no cookie field present in each L2TPv3 data packet)
23.1.2 failover-delay

 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
fail-over <5-60>
```

Parameters

- fail-over <5-60>

<table>
<thead>
<tr>
<th>fail-over &lt;5-60&gt;</th>
<th>Sets the delay interval to re-establish a failed L2TPv3 tunnel (RF-Domain manager/VRRP-master/Cluster-master failover)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;5-60&gt;</td>
<td>Specify a failover delay from 5 - 60 seconds. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

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

```
no
```

Resets the failover interval to its default (5 seconds)
23.1.3 **force-12-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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

`force-12-path-recovery`

**Parameters**

None

**Examples**

```bash
rfs7000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#force-12-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-12-path-recovery
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>Disables the forced detection of servers and gateways behind the L2TPv3 tunnel</td>
</tr>
</tbody>
</table>
23.1.4 `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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

`hello-interval <1-3600>`

**Parameters**

- `hello-interval <1-3600>`

| hello-interval <1-3600> | Configures the interval for L2TPv3 "Hello" keep-alive messages. Specify a value from 1 - 3600 seconds (default is 60 seconds). |

**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 |
23.1.5 no

Negates or reverts L2TPv3 policy settings to default

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [cookie-size|failover-delay|force-12-path-recovery|hello-interval|reconnect-attempts|reconnect-interval|retry-attempts|retry-interval|rx-window-size|tx-window-size]

Parameters

- no [cookie-size|failover-delay|force-12-path-recovery|hello-interval|reconnect-attempts|reconnect-interval|retry-attempts|retry-interval|rx-window-size|tx-window-size]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no cookie-size</td>
<td>Resets the cookie-field size to default (0 - no cookie field present in each L2TPv3 data packet)</td>
</tr>
<tr>
<td>no failover-delay</td>
<td>Resets the failover interval to its default (5 seconds)</td>
</tr>
<tr>
<td>no force-12-path-recovery</td>
<td>Disables the forced detection of servers and gateways behind the L2TPv3 tunnel</td>
</tr>
<tr>
<td>no hello-interval</td>
<td>Resets the “Hello” keep-alive message interval to default (60 seconds)</td>
</tr>
<tr>
<td>no reconnect-attempts</td>
<td>Resets the maximum number of reconnect attempts to default (0 - configures infinite attempts)</td>
</tr>
<tr>
<td>no reconnect-interval</td>
<td>Resets the interval between successive attempts to re-establish a tunnel connection to default (120 seconds)</td>
</tr>
<tr>
<td>no retry-attempts</td>
<td>Resets the maximum number of retransmissions for signalling messages to default (5 attempts)</td>
</tr>
<tr>
<td>no retry-interval</td>
<td>Resets the interval before initiating a retransmission of a L2TPv3 signalling message to default (5 seconds)</td>
</tr>
<tr>
<td>no rx-window-size</td>
<td>Resets the number of packets received without sending an acknowledgment to default (10 packets)</td>
</tr>
<tr>
<td>no tx-window-size</td>
<td>Resets the number of packets transmitted without receiving an acknowledgment to default (10 packets)</td>
</tr>
</tbody>
</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)#
```
The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings after the 'no' commands are executed:

rfs7000-37FAE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
rfs7000-37FAE(config-l2tpv3-policy-L2TPV3Policy1)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cookie-size</td>
<td>Configures the cookie-field size present in each L2TPv3 data packet</td>
</tr>
<tr>
<td>failover-delay</td>
<td>Configures the L2TPv3 tunnel failover delay in seconds</td>
</tr>
<tr>
<td>force-12-path-recovery</td>
<td>Enables the forced detection of servers and gateways behind the L2TPv3 tunnel</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Configures the interval for L2TPv3 &quot;Hello&quot; keep-alive messages</td>
</tr>
<tr>
<td>reconnect-attempts</td>
<td>Configures the maximum number of attempts made to reestablish a tunnel connection</td>
</tr>
<tr>
<td>reconnect-interval</td>
<td>Configures the interval, in seconds, between successive attempts to re-establish a tunnel connection</td>
</tr>
<tr>
<td>retry-attempts</td>
<td>Configures the maximum number of retransmissions for signalling messages from 1 - 10</td>
</tr>
<tr>
<td>retry-interval</td>
<td>Configures the interval, in seconds, before initiating a retransmission of any L2TPv3 signalling message</td>
</tr>
<tr>
<td>rx-window-size</td>
<td>Configures the number of packets received without sending an acknowledgment</td>
</tr>
<tr>
<td>tx-window-size</td>
<td>Configures the number of packets transmitted without receiving an acknowledgment</td>
</tr>
</tbody>
</table>
### 23.1.6 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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
reconnect-attempts <0-8>
```

**Parameters**

- `reconnect-attempts <0-8>`

**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)
23.1.7 reconnect-interval

Configures the interval, in seconds, between two successive attempts to re-establish a failed tunnel connection. Specify a value from 1 - 3600 seconds (default is 120 seconds).

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

reconnect-interval <1-3600>

Parameters

- reconnect-interval <1-3600>

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)
23.1.8 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
retry-attempts <1-10>

Parameters
- retry-attempts <1-10>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retry-attempts &lt;1-10&gt;</td>
<td>Configures the maximum number of attempts made to retransmit signalling messages from 1-10 (default is 5 attempts)</td>
</tr>
</tbody>
</table>

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)
### 23.1.9 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 — AP300, 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, 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. Specify a value from 1 - 250 seconds (default is 5 seconds).</th>
</tr>
</thead>
</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
```

#### Related Commands

- `no` Resets the retry interval to default (5 seconds)
23.1.10 rx-window-size

This command is used to configure the number of signalling packets received without sending an acknowledgment.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
rx-window-size <1-15>

Parameters
rx-window-size <1-15>

Example
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).
23.1.11 tx-window-size

Configures the number of signalling packets transmitted without receiving an acknowledgment

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

tx-window-size <1-15>

Parameters

- tx-window-size <1-15>

| tx-window-size <1-15> | Configures the number of packets transmitted without receiving an acknowledgment. Specify a value from 1 - 15 (default is 10 packets). |

Examples

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)
### 23.2 l2tpv3-tunnel-commands

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:

```plaintext
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 tunnel <TUNNEL-NAME>
```

```plaintext
rfs7000-37FABE(config-profile-default-rfs7000)#l2tpv3 tunnel Tunnel1
rfs7000-37FABE(config-profile_default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

```plaintext
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 23-18</td>
</tr>
<tr>
<td>hostname</td>
<td>Tunnel specific local hostname</td>
<td>page 23-19</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 23-20</td>
</tr>
<tr>
<td>mtu</td>
<td>Configure the mtu size for the tunnel</td>
<td>page 23-21</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 23-22</td>
</tr>
<tr>
<td>peer</td>
<td>Configure the l2tpv3 tunnel peers. At least one peer must be specified</td>
<td>page 23-24</td>
</tr>
<tr>
<td>router-id</td>
<td>Tunnel specific local router ID</td>
<td>page 23-25</td>
</tr>
<tr>
<td>session</td>
<td>Create / modify the specified l2tpv3 session</td>
<td>page 23-26</td>
</tr>
<tr>
<td>use</td>
<td>Set setting to use</td>
<td>page 23-27</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>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>

Table 23.2 summarizes L2TPv3 tunnel configuration commands.
### 23.2.1 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524, NX7500, 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><strong>always</strong></td>
<td>Always establishes a L2TPv3 tunnel from the current device to the NOC controller. This is the default setting.</td>
</tr>
<tr>
<td><strong>cluster-master</strong></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><strong>rf-domain-manager</strong></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 Tunnel1  
establishment-criteria cluster-master
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

**Related Commands**

- **no** Resets to default (always)
23.2.2 hostname

- l2tpv3-tunnel-commands

Configures the tunnel’s local hostname

Supported in the following platforms:
- Access Points — AP300, 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, 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; – Specify the tunnel’s local hostname.</td>
<td></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 | Removes the tunnel’s local hostname |
23.2.3 local-ip-address

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 — AP300, 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, 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
hostname TunnelHost1
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

```
no
```
Resets the tunnel’s local IP address and re-establishes the tunnel
23.2.4 mtu

`l2tpv3-tunnel-commands`

Configures the Maximum Transmission Unit (MTU) size for this tunnel. This value determines the packet size transmitted over this tunnel.

Supported in the following platforms:
- Access Points — AP300, 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, 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. Specify a value from 128 - 1460 bytes (default is 1460 bytes).</th>
</tr>
</thead>
</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) |
23.2.5 **no**

- **l2tpv3-tunnel-commands**

Negates or reverts a L2TPv3 tunnel settings to default

Supported in the following platforms:

- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [establishment-criteria|hostname|local-ip-address|mtu|peer|router-id|session|use]
```

**Parameters**

- `no [establishment-criteria|hostname|local-ip-address|mtu|peer|router-id|session|use]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>establishment-criteria</td>
<td>Resets the tunnel’s establishment criteria to default</td>
</tr>
<tr>
<td>no hostname</td>
<td>Removes the tunnel’s local hostname</td>
</tr>
<tr>
<td>no local-ip-address</td>
<td>Resets the tunnel’s local IP address and re-establishes the tunnel</td>
</tr>
<tr>
<td>no mtu</td>
<td>Resets the MTU size for this tunnel to default (1460 bytes)</td>
</tr>
<tr>
<td>no peer</td>
<td>Removes the peer configured for this tunnel</td>
</tr>
<tr>
<td>no router-id</td>
<td>Removes the tunnel’s router ID</td>
</tr>
<tr>
<td>no session</td>
<td>Removes a session</td>
</tr>
<tr>
<td>no use</td>
<td>Removes the L2TPv3 policy associated with a tunnel and reverts to the default tunnel policy</td>
</tr>
</tbody>
</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)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>establishment-criteria</td>
<td>Configures a L2TPv3 tunnel’s establishment criteria</td>
</tr>
<tr>
<td>hostname</td>
<td>Configures the tunnel’s local hostname</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Configures the tunnel’s source IP address</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the MTU size for this tunnel</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the tunnel’s peers</td>
</tr>
<tr>
<td>router-id</td>
<td>Configures the tunnel’s local router ID</td>
</tr>
<tr>
<td>session</td>
<td>Creates/modifies specified L2TPv3 session</td>
</tr>
<tr>
<td>use</td>
<td>Associates a specified L2TPv3 tunnel policy with a L2TPv3 tunnel</td>
</tr>
</tbody>
</table>
## 23.2.6 peer

**l2tpv3-tunnel-commands**

Configures the L2TPv3 tunnel’s peers. At least one peer must be specified.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

### Syntax

```plaintext
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>|any]} {ipsec-secure|udp} 
peer <1-2> {udp} {ipsec-secure|port <1-65535>} 
```

### Parameters

- **peer <1-2> {hostname [any]} {ipsec-secure|router-id|udp}**
  - Configures the tunnel’s peer ID from 1 - 2
  - **Note:** At any time the tunnel is established with only one peer.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Optional. Configures the peers’ hostname. The hostname options are:</td>
</tr>
<tr>
<td>[&lt;HOSTNAME&gt;</td>
<td>any]</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</td>
<td>After specifying the peer hostname, optionally specify the IPSec settings:</td>
</tr>
<tr>
<td>{gw [&lt;IP&gt;</td>
<td>&lt;WORD&gt;]}</td>
</tr>
<tr>
<td></td>
<td>• gw – Optional. Configures IPSec gateway IP address or hostname</td>
</tr>
<tr>
<td></td>
<td>• &lt;IP&gt; – Configures IPSec gateway’s IP address</td>
</tr>
<tr>
<td></td>
<td>• &lt;WORD&gt; – Configures IPSec gateway’s hostname</td>
</tr>
<tr>
<td>router-id</td>
<td>After specifying the peer hostname, optionally specify router ID settings:</td>
</tr>
<tr>
<td>[&lt;IP&gt;</td>
<td>&lt;WORD&gt;</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>
<tr>
<td>udp</td>
<td>After specifying the peer hostname, optionally specify UDP settings:</td>
</tr>
<tr>
<td>{ipsec-secure gw</td>
<td>port</td>
</tr>
<tr>
<td></td>
<td>• UDP – Optional. Configures UDP encapsulation (default encapsulation is IP)</td>
</tr>
<tr>
<td></td>
<td>• ipsec-secure gw – Optional. Enables auto IPSec</td>
</tr>
<tr>
<td></td>
<td>• port &lt;1-65535&gt; {ipsec-secure} – 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.</td>
</tr>
</tbody>
</table>
### L2TPv3-POLICY 23 - 25

#### peer <1-2> {ip-address <IP>} {hostname|ipsec-secure|router-id|udp}

<table>
<thead>
<tr>
<th>peer &lt;1-2&gt;</th>
<th>Configures the tunnel’s peer ID from 1 - 2. At any time the tunnel is established with only one peer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address &lt;IP&gt;</td>
<td>Optional. Configures the peer’s IP address in the A.B.C.D format</td>
</tr>
</tbody>
</table>
| hostname [<FQDN>|any] | After specifying the peer IP address, optionally specify the peer’s hostname: Optional. Configures the peers’ hostname. The hostname options are:  
  - <FQDN> – Specifies the hostname 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 IPSec gateway IP address or hostname  
    - <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>]}

<table>
<thead>
<tr>
<th>peer &lt;1-2&gt;</th>
<th>Configures the tunnel’s peer ID from 1 - 2. At any time the tunnel is established with only one peer.</th>
</tr>
</thead>
</table>
| ipsec-secure {gw [<IP>|<WORD>]} | Optional. Enables auto IPSec for this peer  
  - gw – Optional. Configures IPSec gateway IP address or hostname  
    - <IP> – Configures IPSec gateway’s IP address  
    - <WORD> – Configures IPSec gateway’s hostname |

#### peer <1-2> {router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}

<table>
<thead>
<tr>
<th>peer &lt;1-2&gt;</th>
<th>Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec-secure (gw [&lt;IP&gt;</td>
<td>&lt;WORD&gt;])</td>
</tr>
</tbody>
</table>
|                                                                      | • ipsec-secure – Optional. Enables auto IPSec  
|                                                                      | • gw – Optional. Configures IPSec gateway IP address or hostname  
|                                                                      | • <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. |
| peer <1-2> {udp} {ipsec-secure|port <1-65535>}                  | Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.                                                                                                            |
| udp {ipsec-secure|port <1-65535>|ipsec-secure}                                              | Optional. Configures UDP encapsulation for this tunnel’s peer (default encapsulation is IP)                                                                                                                      |
|                                                                      | • ipsec-secure – Optional. Configures IPSec gateway on this peer UDP port  
|                                                                      | • 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 tunnellpeer1 udp port 100
```

```
rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
  l2tpv3 tunnel Tunnel1
    peer 2 hostname tunnellpeer1 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
23.2.7 router-id

**l2tpv3-tunnel-commands**

Configures the tunnel’s local router ID

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
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**

```plaintext
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 tunnellpeer1 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 |
### 23.2.8 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP811X, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
    vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session</code> &lt;L2TPV3-SESSION-NAME&gt;</td>
<td>Configures this session’s name</td>
</tr>
<tr>
<td><code>pseudowire-id</code> &lt;1-4294967295&gt;</td>
<td>Configures the pseudowire ID for this session from 1- 4204067295</td>
</tr>
<tr>
<td><code>traffic-source vlan</code> &lt;VLAN-ID-RANGE&gt;</td>
<td>Configures VLAN as the traffic source for this tunnel</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;VLAN-ID-RANGE&gt;</code> – 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><code>native-vlan</code> &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>- <code>&lt;1-4094&gt;</code> – Specify the native VLAN ID from 1- 4094.</td>
</tr>
</tbody>
</table>

**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
tunnel1peer1session1 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 tunnellpeer1 udp port 100
    session tunnellpeer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
    router-id 2000
    establishment-criteria cluster-master
```

**Related Commands**

```
no
```

Removes a session
23.2.9 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 — AP300, 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, 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
  - 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>............ 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>............ 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.

Examples

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
23.3 l2tpv3-manual-session-commands

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)#
```

```
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)#
```

Table 23.3 summarizes L2TPv3 manual session configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-cookie</td>
<td>Configures the manual session’s local cookie field size</td>
<td>page 23-31</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Configures the manual session’s local source IP address</td>
<td>page 23-32</td>
</tr>
<tr>
<td>local-session-id</td>
<td>Configures the manual session’s local session ID</td>
<td>page 23-33</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the MTU size for the manual session tunnel</td>
<td>page 23-34</td>
</tr>
<tr>
<td>no</td>
<td>Negates or reverts L2TPv3 manual session commands to default</td>
<td>page 23-22</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the manual session’s peers</td>
<td>page 23-37</td>
</tr>
<tr>
<td>remote-cookie</td>
<td>Configures the remote cookie for the manual session</td>
<td>page 23-38</td>
</tr>
<tr>
<td>remote-session-id</td>
<td>Configures the manual session’s remote session ID</td>
<td>page 23-39</td>
</tr>
<tr>
<td>traffic-source</td>
<td>Configures the traffic source tunneled by the manual session</td>
<td>page 23-40</td>
</tr>
</tbody>
</table>
23.3.1 local-cookie

**l2tpv3-manual-session-commands**

Configures the local cookie field size for the manual session

Supported in the following platforms:
- Access Points — AP300, 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, 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
23.3.2 local-ip-address

- l2tpv3-manual-session-commands

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 — AP300, 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, 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
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)#

Related Commands
- **no**
  Resets the manual session's local source IP address. This re-establishes the session.
23.3.3 local-session-id

- l2tpv3-manual-session-commands

Configures the manual session's local session ID

Supported in the following platforms:

- Access Points — AP300, 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, 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

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

rfs7000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

Related Commands

| no | Removes the manual session's local session ID |
23.3.4 mtu

**l2tpv3-manual-session-commands**

Configures the *Maximum Transmission Unit* (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 — AP300, 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, 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)
23.3.5 **no**

Negates or reverts L2TPv3 manual session settings to default

Supported in the following platforms:
- **Access Points** — AP300, 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, 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 [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|
  remote-session-id|traffic-source]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no local-cookie</td>
<td>Removes the local cookie size configured for a manual session</td>
</tr>
<tr>
<td>no local-ip-address</td>
<td>Resets the manual session’s local source IP address and re-establishes the tunnel</td>
</tr>
<tr>
<td>no local-session-id</td>
<td>Removes the manual session’s local session ID</td>
</tr>
<tr>
<td>no mtu</td>
<td>Resets the manual session’s MTU size to default (1460 bytes)</td>
</tr>
<tr>
<td>no peer</td>
<td>Removes the peer configuration from this tunnel</td>
</tr>
<tr>
<td>no remote-cookie</td>
<td>Removes the remote cookie field size</td>
</tr>
<tr>
<td>no remote-session-id</td>
<td>Removes the manual session’s remote session ID</td>
</tr>
<tr>
<td>no traffic-source</td>
<td>Removes the configured traffic source</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the manual session ‘test’ settings before the ‘no’ commands are executed:

```bash
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)#
```

```bash
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)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-cookie</td>
<td>Configures the local cookie field size for the manual session</td>
</tr>
<tr>
<td>local-ip-address</td>
<td>Configures the manual session's local source IP address</td>
</tr>
<tr>
<td>local-session-id</td>
<td>Removes the manual session's local session ID</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the manual session's MTU size</td>
</tr>
<tr>
<td>peer</td>
<td>Configures the manual session's peers</td>
</tr>
<tr>
<td>remote-cookie</td>
<td>Configures the manual session's remote cookie field size</td>
</tr>
<tr>
<td>remote-session-id</td>
<td>Configures the manual session's remote session ID</td>
</tr>
<tr>
<td>traffic-source</td>
<td>Configures the traffic source tunneled in this session</td>
</tr>
</tbody>
</table>
23.3.6 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 — AP300, 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, 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. 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
## 23.3.7 remote-cookie

**l2tpv3-manual-session-commands**

Configures the manual session’s remote cookie field size

Supported in the following platforms:
- Access Points — AP300, 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, 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
  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**

- `no` Removes the manual session’s remote cookie field size
23.3.8 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 — AP300, 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, 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
23.3.9 traffic-source

Configures the traffic source tunneled by this session

Supported in the following platforms:

- Access Points — AP300, 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, 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>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>

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
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
- `vrrp-state-check` Publish interface via OSPF only if the interface VRRP state is not BACKUP

- `clrscr` Clears the display screen
- `commit` Commit all changes made in this session
- `do` Run commands from Exec mode
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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-profile default-rfs7000-router-ospf)#
## 24.1 router-mode

Table 24.1 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 24-4</td>
</tr>
<tr>
<td>auto-cost</td>
<td>Specifies the reference bandwidth in terms of Mbits per second</td>
<td>page 24-13</td>
</tr>
<tr>
<td>default-information</td>
<td>Controls the distribution of default information</td>
<td>page 24-14</td>
</tr>
<tr>
<td>ip</td>
<td>Configures Internet Protocol (IP) default gateway priority</td>
<td>page 24-15</td>
</tr>
<tr>
<td>network</td>
<td>Defines OSPF network settings</td>
<td>page 24-16</td>
</tr>
<tr>
<td>ospf</td>
<td>Enables OSPF</td>
<td>page 24-17</td>
</tr>
<tr>
<td>passive</td>
<td>Specifies the configured OSPF interface as passive interface</td>
<td>page 24-18</td>
</tr>
<tr>
<td>redistribute</td>
<td>Specifies the route types redistributed by OSPF</td>
<td>page 24-19</td>
</tr>
<tr>
<td>route-limit</td>
<td>Specifies the limit for the number of routes managed by OSPF</td>
<td>page 24-20</td>
</tr>
<tr>
<td>router-id</td>
<td>Specifies the router ID for OSPF</td>
<td>page 24-21</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>Publishes interface via OSPF based on VRRP status</td>
<td>page 24-22</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its defaults</td>
<td>page 24-23</td>
</tr>
</tbody>
</table>
24.1.1 area

Configures OSPF network area (OSPF enabled interfaces) settings

Table 24.2 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 24-5</td>
</tr>
<tr>
<td>OSPF-area-mode</td>
<td>Summarizes OSPF area configuration commands</td>
<td>page 24-7</td>
</tr>
</tbody>
</table>
### 24.1.1.1 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 defined as: stub area, totally-stub, non-stub, nssa, totally nssa. Each of these area types have 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 — AP300, 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

**Syntax**

```
area [<0-4294967295>|<IP>]
```

**Parameters**

- area [<0-4294967295>|<IP>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>Defines an OSPF area in the form of a 32 bit integer. Specify the value from 0 - 4294967295.</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Defines an OSPF area in the form of an IP address. Specify the IP address.</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><em>no</em></td>
<td>Removes area configuration settings</td>
</tr>
</tbody>
</table>
24.1.1.2 OSPF-area-mode

Table 24.3 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 24-8</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the authentication scheme used for the OSPF area</td>
<td>page 24-10</td>
</tr>
<tr>
<td>range</td>
<td>Specifies the routes matching address/mask for summarization</td>
<td>page 24-11</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its defaults</td>
<td>page 24-12</td>
</tr>
</tbody>
</table>
24.1.1.2.1 area-type

OSPF-area-mode

Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA

Areas can 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** — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- **Wireless Controllers** — RFS4000, RFS6000, RFS7000
- **Service Platforms** — NX4500, NX4524, NX6500, NX6524

**Syntax**

```plaintext
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]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</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 <em>Stubby Area</em> (STUB)</td>
</tr>
<tr>
<td>default-cost &lt;0-16777215&gt;</td>
<td>Specifies the default summary cost that will be advertised, if the OSPF area is a STUB or NSSA</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 <em>Link State Advertisements</em> (LSAs) into type-5 LSAs</td>
</tr>
</tbody>
</table>
### Examples

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes configured area-type settings</td>
</tr>
</tbody>
</table>
24.1.1.2.2 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 — AP300, 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

Syntax

authentication [message-digest|simple-password]

Parameters

- authentication [message-digest|simple-password]

| message-digest | Configures the message-digest (MD-5) authentication scheme |
| simple-password | Configures the simple password authentication scheme |

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
24.1.1.2.3 range

**OSPF-area-mode**

Specifies a range of addresses for routes matching address/mask for OSPF summarization.

Supported in the following platforms:
- Access Points — AP300, 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

**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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> This command is applicable for a <em>Area Border Router</em> (ABR) only.</td>
<td></td>
</tr>
</tbody>
</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 |
24.1.1.2.4 no

Negates a command or set its defaults

Supported in the following platforms:
- Access Points — AP300, 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

**Syntax**

```plaintext
no [area-type|authentication|range]
```

**Parameters**

- `no [area-type|authentication|range]`

**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)#
```

```plaintext
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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-type</td>
<td>Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the authentication scheme used for an OSPF area</td>
</tr>
<tr>
<td>range</td>
<td>Specifies the routes matching address/mask for summarization</td>
</tr>
</tbody>
</table>
24.1.2 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’ to configure default metrics calculation based on interface type.

Supported in the following platforms:
- Access Points — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524

**Syntax**

`auto-cost reference-bandwidth <1-4294967>`

**Parameters**

- `auto-cost reference-bandwidth <1-4294967>`

<table>
<thead>
<tr>
<th>reference-bandwidth &lt;1-4294967&gt;</th>
<th>Defines the reference bandwidth in Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <code>&lt;1-4294967&gt;</code> – Specify the reference bandwidth value from 1 - 4294967.</td>
</tr>
</tbody>
</table>

**Examples**

```
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

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
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
24.1.3 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** — AP300, 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

**Syntax**

```plaintext
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>metric-type [1</td>
<td>2]</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
24.1.4 ip

**router-mode**

Configures IP default gateway priority

Supported in the following platforms:

- Access Points — AP300, 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

**Syntax**

ip default-gateway priority <1-8000>

**Parameters**

- **ip default-gateway priority <1-8000>**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-gateway priority &lt;1-8000&gt;</td>
<td>Configures the default gateway priority</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
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**

- **no** Removes default gateway priority settings
24.1.5 network

Assigns networks to specified areas (defines the OSPF interfaces and their associated area IDs)

Supported in the following platforms:

- Access Points — AP300, 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

Syntax

network <IP/M> area [<0-4294967295>|<IP>]

Parameters

- network <IP/M> area [<0-4294967295>|<IP>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP/M&gt;</td>
<td>Specifies an OSPF network address/mask value. Defines networks (IP addresses and mask) participating in OSPF.</td>
</tr>
<tr>
<td>area</td>
<td>Specifies an OSPF area, associated with the OSPF address range, in one of the following formats:</td>
</tr>
<tr>
<td>[0-4294967295]</td>
<td>- &lt;0-4294967295&gt; – Specifies a 32 bit OSPF area ID from 0 - 4294967295</td>
</tr>
<tr>
<td>[&lt;IP&gt;]</td>
<td>- &lt;IP&gt; – Defines an OSPF area ID in the form of an IPv4 address</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the OSPF network to area ID association</td>
</tr>
</tbody>
</table>
24.1.6 ospf

Enables OSPF routing on a profile or device

Supported in the following platforms:

- Access Points — AP300, 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

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
routerr 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
24.1.7 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 — AP300, 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

**Syntax**

```
passive [<WORD>|all|vlan <1-4094>]
```

**Parameters**

- passive [<WORD>|all|vlan <1-4094>]

<table>
<thead>
<tr>
<th>&lt;WORD&gt;</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables the OSPF passive mode on all the L3 interfaces</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Enables the OSPF passive mode on the specified VLAN interface</td>
</tr>
</tbody>
</table>

| <1-4094> | Specify the VLAN interface ID from 1 - 4094. |

**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
24.1.8 redistribute

Specifies the route types redistributed by OSPF

Supported in the following platforms:
- Access Points — AP300, 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

Syntax
redistribute [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>connected</td>
<td>Redistributes all connected interface routes by OSPF</td>
</tr>
<tr>
<td>kernel</td>
<td>Redistributes all routes that are neither connected, nor static, nor dynamic</td>
</tr>
<tr>
<td>static</td>
<td>Redistributes static routes by OSPF</td>
</tr>
</tbody>
</table>
| metric <0-16777214> | The following keywords are common to the ‘connected’, ‘kernel’, and ‘static’ parameters:  
  - metric <0-16777214> – Optional. Specifies the OSPF metric value for redistributed routes.  
  - <0-16777214> – Specify a value from 0 - 16777214. |
| metric-type [1|2] | The following keywords are common to the ‘connected’, ‘kernel’, and ‘static’ parameters:  
  - metric-type [1|2] – Optional. Sets the OSPF exterior metric type for redistributed routes  
  - 1 – Sets the OSPF external type 1 metrics  
  - 2 – Sets the OSPF external type 2 metrics |

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
24.1.9 route-limit

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 — AP300, 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

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 Link State Advertisements (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. 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. 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. 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-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
24.1.10 router-id

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 — AP300, 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

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
24.1.11 `vrrp-state-check`

**router-mode**

Publishes interface via OSPF based on *Virtual Router Redundancy Protocol* (VRRP) status

VRRP provides automatic assignments 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:

- Access Points — AP300, 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

**Syntax**

`vrrp-state-check`

**Parameters**

- `vrrp-state-check`

| vrrp-state-check | Publishes an interface via OSPF based on VRRP status |

**Examples**

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#vrrp-state-check
```

Disable and enable OSPF feature for this command to take effect

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#
```

```
rfs7000-37FABE(config-profile default-rfs7000-router-ospf)#show context include-factory
router ospf
  ospf enable
  no router-id
  no auto-cost reference-bandwidth
  no default-information originate
  no passive all
  vrrp-state-check
  route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
  ip default-gateway priority 7000
```

**Related Commands**

- `no` Disables the publishing of an interface via OSPF based on VRRP status
24.1.12 no

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — AP300, 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

Syntax

no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|route-limit|router-id|vrrp-state-check]

Parameters

- no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|route-limit|router-id|vrrp-state-check]

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:

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)#

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:

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)#
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Configures OSPF network areas (OSPF enables interfaces)</td>
</tr>
<tr>
<td>auto-cost</td>
<td>Configures the reference bandwidth in terms of megabits per second</td>
</tr>
<tr>
<td>default-information</td>
<td>Controls the distribution of default route information</td>
</tr>
<tr>
<td>ip</td>
<td>Configures IP default gateway priority</td>
</tr>
<tr>
<td>network</td>
<td>Assigns networks to specified areas</td>
</tr>
<tr>
<td>ospf</td>
<td>Enables OSPF</td>
</tr>
<tr>
<td>passive</td>
<td>Configures a specified OSPF interface as passive</td>
</tr>
<tr>
<td>redistribute</td>
<td>Specifies the route types redistributed by OSPF</td>
</tr>
<tr>
<td>route-limit</td>
<td>Limits the number of routes managed by OSPF</td>
</tr>
<tr>
<td>router-id</td>
<td>Specifies the router ID for OSPF</td>
</tr>
<tr>
<td>vrrp-state-check</td>
<td>Publishes interface via OSPF based on VRRP status</td>
</tr>
</tbody>
</table>
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 policies facilitate 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
rfs7000-37FABE(config)#
```

```
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)#
```
25.1 routing-policy-commands

Table 25.1 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/disables PBR for locally generated packets</td>
<td>page 25-3</td>
</tr>
<tr>
<td>logging</td>
<td>Enables/disables logging for a specified route map</td>
<td>page 25-4</td>
</tr>
<tr>
<td>route-map</td>
<td>Creates a route map entry</td>
<td>page 25-5</td>
</tr>
<tr>
<td>use</td>
<td>Defines default settings to use</td>
<td>page 25-15</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its defaults</td>
<td>page 25-16</td>
</tr>
</tbody>
</table>
25.1.1 apply-to-local-packets

Enables/disables 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 — AP300, 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, 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>
```
25.1.2 logging

```
routing-policy-commands

Enables/disables 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600
```

**Syntax**

```
logging
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-routing-policy-testpolicy)#logging
rfs7000-37FABE(config-routing-policy-testpolicy)#show context
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>
25.1.3 route-map

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-map 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
route-map <1-100>
```

**Parameters**

- route-map <1-100>

<table>
<thead>
<tr>
<th>route-map &lt;1-100&gt;</th>
<th>Creates a route map entry and enters the route map configuration mode. Specify a precedence value from 1-100.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Lower the sequence number, higher is the precedence.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

```
rfs7000-37FABE(config-routing-policy-testpolicy)#route-map 1
```

```
rfs7000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
logging
route-map 1
```

```
rfs7000-37FABE(config-routing-policy-testpolicy)#route-map 1
```

```
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 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-route-map-1)#
```

**Related Commands**

| **no** | Removes a route map |
25.1.4 route-map-mode

Table 25.2 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 25-8</td>
</tr>
<tr>
<td>fallback</td>
<td>Configures a fallback to the next destination</td>
<td>page 25-9</td>
</tr>
<tr>
<td>mark</td>
<td>Marks action clause for packets satisfying match criteria</td>
<td>page 25-10</td>
</tr>
<tr>
<td>match</td>
<td>Sets match clauses for the route map</td>
<td>page 25-11</td>
</tr>
<tr>
<td>next-hop</td>
<td>Sets the next hop for packets satisfying match criteria</td>
<td>page 25-13</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 25-14</td>
</tr>
</tbody>
</table>
25.1.4.1 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6524, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwan1]

Parameters

- default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwan1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</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</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Specifies the PPPoE interface</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Specifies a VLAN interface ID from 1 - 4094</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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes default next hop router settings</td>
</tr>
</tbody>
</table>
**25.1.4.2 fallback**

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** — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
fallback
```

**Parameters**

None

**Examples**

```
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#fallback
```

**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>
25.1.4.3 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 — AP300, 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, 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. Specify a DSCP value from 0 - 63.</th>
</tr>
</thead>
</table>

**Examples**

```bash
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context route-map 1
default-next-hop wwan1
  mark ip dscp 7
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

**Related Commands**

```
no
```

Disables marking of IP packets
25.1.4.4 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

### Syntax

```plaintext
match [incoming-interface|ip|ip-access-list|wireless-client-role|wlan]

match incoming-interface [<ROUTER-IF-NAME>|pppoel|vlan <1-4094>|wwan1]
match ip dscp <0-63>
match ip-access-list <IP-ACCESS-LIST-NAME>
match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>
match wlan <WLAN-NAME>
```

### Parameters

- **match incoming-interface [<ROUTER-IF-NAME>|pppoel|vlan <1-4094>|wwan1]**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>incoming-interface</td>
<td>Sets the incoming SVI match clause. Specify an interface name.</td>
</tr>
<tr>
<td>&lt;ROUTER-IF-NAME&gt;</td>
<td>Specifies the layer 3 interface name (route interface)</td>
</tr>
</tbody>
</table>
match ip dscp <0-63>

Example:
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#match incoming-interface pppoe1

Related Commands:
no

Disables match clause settings for this route map.
25.1.4.5 next-hop

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwlan1]

Parameters

- next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|vlan <1-4094>|wwlan1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next-hop</td>
<td>Sets the next hop (primary and secondary) for packets satisfying match criteria</td>
</tr>
<tr>
<td>&lt;IP&gt;</td>
<td>Specifies the primary and secondary next hop router’s IP address</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>Specifies the layer 3 Interface name (router interface)</td>
</tr>
<tr>
<td>pppoe1</td>
<td>Specifies the PPP over Ethernet interface</td>
</tr>
<tr>
<td>vlan &lt;1-4094&gt;</td>
<td>Specifies the VLAN interface. Specify a VLAN ID from 1 - 4094. The VLAN interface should be a DHCP client.</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)#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
rfs7000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

- `no` Disables the next hop router settings
25.1.4.6 no

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [default-next-hop|fallback|mark|match|next-hop]

Parameters

- no [default-next-hop|fallback|mark|match|next-hop]

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)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-next-hop</td>
<td>Sets the next hop for packets satisfying match criteria</td>
</tr>
<tr>
<td>fallback</td>
<td>Configures a fallback to the next destination</td>
</tr>
<tr>
<td>mark</td>
<td>Marks an action for a route map</td>
</tr>
<tr>
<td>match</td>
<td>Sets match clauses for a route map</td>
</tr>
<tr>
<td>next-hop</td>
<td>Sets the next hop for packets satisfying match criteria</td>
</tr>
</tbody>
</table>
25.1.5 use

- **routing-policy-commands**

Uses *Critical Resource Management* (CRM) to monitor link status

Supported in the following platforms:
- Access Points — AP300, 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, 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
25.1.6 **no**

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [apply-to-local-packets|logging|route-map|use]
```

**Parameters**

```
- no [apply-to-local-packets|logging|route-map|use]
```

<table>
<thead>
<tr>
<th>no &lt;PARAMETER&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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply-to-local-packets</td>
<td>Enables/disables PBR for locally generated packets</td>
</tr>
<tr>
<td>logging</td>
<td>Enables logging for a specified route map</td>
</tr>
<tr>
<td>route-map</td>
<td>Creates a route map entry and enters the route map configuration mode</td>
</tr>
<tr>
<td>use</td>
<td>Uses CRM to monitor the status of a link</td>
</tr>
</tbody>
</table>
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:

```
<DEVICE>(config)#aaa-tacacs-policy <POLICY-NAME>
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
26.1 aaa-tacacs-policy

AAA-TACACS-POLICY

Table 26.1 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 26-3</td>
</tr>
<tr>
<td>authentication</td>
<td>Configures TACACS authentication parameters</td>
<td>page 26-6</td>
</tr>
<tr>
<td>authorization</td>
<td>Configures TACACS authorization parameters</td>
<td>page 26-9</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or sets its default</td>
<td>page 26-12</td>
</tr>
</tbody>
</table>
### 26.1.1 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 — AP300, 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, 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>]} {port <1-65535>}
accounting server <1-2> timeout <3-5> {attempts <1-3>}
```

**Parameters**
- **accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}**

<table>
<thead>
<tr>
<th>access-method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Configures TACACS accounting for all access modes</td>
</tr>
<tr>
<td>console</td>
<td>Configures TACACS accounting for console access only</td>
</tr>
<tr>
<td>ssh</td>
<td>Configures TACACS accounting for SSH access only</td>
</tr>
<tr>
<td>telnet</td>
<td>Configures TACACS accounting for Telnet access only</td>
</tr>
</tbody>
</table>

- **accounting [auth-fail|commands|session]**

| 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. |
### accounting server preference

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticated-server-host</td>
<td>Sets the authentication server as the accounting server. This is the default setting. 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 preference <1-2> retry-timeout-factor <50-200>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server &lt;1-2&gt;</td>
<td>Configures an accounting server. Up to 2 accounting servers can be configured</td>
</tr>
<tr>
<td>retry-timeout-factor &lt;50-200&gt;</td>
<td>Sets the scaling factor for retry timeouts</td>
</tr>
<tr>
<td></td>
<td>• &lt;50-200&gt; – Specify a value from 50 - 200. The default is 150.</td>
</tr>
<tr>
<td></td>
<td>A value of 100 indicates the time gap between two consecutive retries remains the same irrespective of the number of retries.</td>
</tr>
<tr>
<td></td>
<td>A value lesser than 100 indicates the time gap between two consecutive retries reduces with each successive retry.</td>
</tr>
<tr>
<td></td>
<td>A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry.</td>
</tr>
</tbody>
</table>

### accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET> | 2 <SECRET> | <SECRET>]} {port <1-65535>}

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server &lt;1-2&gt;</td>
<td>Configures an accounting server. Up to 2 accounting servers can be configured</td>
</tr>
<tr>
<td>host [IP/HOSTNAME]</td>
<td>Configures the accounting server’s IP address or hostname</td>
</tr>
<tr>
<td>secret [0 &lt;SECRET&gt;</td>
<td>2 &lt;SECRET&gt;</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Optional. Configures the accounting server port (the port used to connect to the accounting server)</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-65535&gt; – Specify the TCP accounting port number from 1 - 65535. The default port is 49.</td>
</tr>
</tbody>
</table>
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. |
| 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. |

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 |
### 26.1.2 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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
authentication [access-method|directed-request|server|service]

authentication access-method [all|console|ssh|telnet|web] {(console|ssh|telnet|web)}

authentication directed-request

authentication server <1-2> [host|retry-timeout-factor|timeout]
authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}
authentication server <1-2> retry-timeout-factor <50-200>
authentication server <1-2> timeout <3-60> {attempts <1-10>}

authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}
```

**Parameters**

- **access-method**
  - all
    - Configure access modes for TACACS authentication. The options are: console, SSH, Telnet, Web, and all
  - 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
AAA-TACACS-POLICY 26 - 7

<table>
<thead>
<tr>
<th>secret [0 &lt;SECRET&gt;]</th>
<th>Configures the secret key used to authenticate with the TACACS server</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 &lt;SECRET&gt;[&lt;SECRET&gt;]</td>
<td>- 0 &lt;SECRET&gt; – Configures a clear text secret</td>
</tr>
<tr>
<td></td>
<td>- 2 &lt;SECRET&gt; – Configures an encrypted secret</td>
</tr>
<tr>
<td></td>
<td>- &lt;SECRET&gt; – Specify the secret key. The shared key should not exceed 127 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port &lt;1-65535&gt;</th>
<th>Optional. Specifies the port used to connect to the TACACS server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &lt;1-65535&gt; – Specify a value for the TCP authentication port from 1 - 65535. The default port is 49.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>server &lt;1-2&gt;</th>
<th>Configures a TACACS authentication server. Up to 2 TACACS servers can be configured</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &lt;1-2&gt; – Specify the TACACS server index from 1 - 2.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>retry-timeout-factor &lt;50-200&gt;</th>
<th>Configures timeout scaling between two consecutive TACACS authentication retries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &lt;50-200&gt; – Specify the scaling factor from 50 - 200. The default is 100.</td>
</tr>
<tr>
<td></td>
<td>A value of 100 indicates the interval between consecutive retries remains the same irrespective of the number of retries.</td>
</tr>
<tr>
<td></td>
<td>A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry.</td>
</tr>
<tr>
<td></td>
<td>A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>server &lt;1-2&gt;</th>
<th>Configures a TACACS authentication server. Up to 2 TACACS servers can be configured</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &lt;1-2&gt; – Specify the TACACS server index from 1 - 2.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>timeout &lt;3-60&gt;</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &lt;3-60&gt; – Specify a value from 3- 60 seconds. The default is 3 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>attempts &lt;1-10&gt;</th>
<th>Optional. Indicates the number of retry attempts to make before giving up</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &lt;1-10&gt; – Specify a value from 1 -10. The default is 3.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>authentication service &lt;SERVICE-NAME&gt;</th>
<th>{protocol &lt;AUTHENTICATION-PROTO-NAME&gt;}</th>
<th>Configures the TACACS authentication service name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>protocol &lt;AUTHENTICATION-PROTO-NAME&gt;</th>
<th>Optional. Specify the authentication protocol used with this TACACS policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> A maximum of five entries is allowed.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Resets values or disables commands</td>
</tr>
</tbody>
</table>
26.1.3 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 — AP300, 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, 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>]} {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

| allow-privileged-commands | Allows privileged commands execution without command authorization. This option is disabled by default. |

- authorization 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 a TACACS authorization server. Up to 2 TACACS servers can be configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-2&gt;</td>
<td>Specify the TACACS server index from 1 - 2.</td>
</tr>
</tbody>
</table>

| host <IP/HOSTNAME> | Sets the TACACS server’s IP address or hostname |

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| secret [0 <SECRET>| 2 <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.                                 |
| authorization server <1-2> retry-timeout-factor <50-200>              | Configures the scaling of timeouts between consecutive TACACS authorization 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 authorization server. Up to 2 TACACS servers can be configured  
  • <1-2> – Specify the TACACS server's index from 1 - 2.                                                                       |
| retry-timeout-factor <50-200>                                        | Configures the scaling of timeouts between consecutive TACACS authorization 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. |
| authorization server <1-2> timeout <3-5> attempts <1-3>               | Configures a TACACS authorization server. Up to 2 TACACS servers can be configured  
  • <1-2> – Specify the TACACS server's index from 1 - 2.                                                                       |
| server <1-2>                                                         | Configures a TACACS authorization server. Up to 2 TACACS servers can be configured  
  • <1-2> – Specify the TACACS server's index from 1 - 2.                                                                       |
| timeout <3-5>                                                        | 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.  
  • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.                                                        |
| attempts <1-3>                                                       | Optional. Indicates the number of retry attempts to make before giving up  
  • <1-3> – Specify a value from 1 - 3. The default is 3.                                                                            |
| authorization server preference [authenticated-server-host|authenticated-server-number|none] | Configures the authorization server preference  
  **authenticated-server-host**  
  This parameter indicates the same server is used for authentication and authorization+. The server is referred to by its hostname.  
  **authenticated-server-number**  
  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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets values or disables commands</td>
</tr>
</tbody>
</table>
26.1.4 no

Negates a AAA TACACS policy command or sets its default

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
no [accounting|authentication|authorization]

Parameters
- no <PARAMETER>

| no <PARAMETER> | Provide the parameters needed to reset or disable the desired AAA-TACACS policy setting. |

Examples
The following example shows the AAA-TACACS policy ‘test’ settings before the ‘no’ commands are executed:

```
rsf7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
  accounting server preference authorized-server-number
  authentication directed-request
  authorization allow-privileged-commands
  accounting auth-fail
  accounting commands
rsf7000-37FABE(config-aaa-tacacs-policy-test)#
```

```
rsf7000-37FABE(config-aaa-tacacs-policy-test)#no authentication directed-request
rsf7000-37FABE(config-aaa-tacacs-policy-test)#no accounting auth-fail
rsf7000-37FABE(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:

```
rsf7000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
  accounting server preference authorized-server-number
  accounting commands
rsf7000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Configures TACACS accounting parameters</td>
</tr>
<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`
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
  - 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
do
end
end
exit
exit
help
help
revert
revert
service
service
show
show
write
write
```

```
rfs7000-37FABE(config-meshpoint-test)#
```
Table 27.1 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 27-4</td>
</tr>
<tr>
<td>beacon-format</td>
<td>Configures the beacon format for the meshpoint AP</td>
<td>page 27-5</td>
</tr>
<tr>
<td>control-vlan</td>
<td>Configures the VLAN where meshpoint control traffic traverses</td>
<td>page 27-6</td>
</tr>
<tr>
<td>data-rates</td>
<td>Configures the data rates supported per frequency band</td>
<td>page 27-7</td>
</tr>
<tr>
<td>description</td>
<td>Configures a human friendly description for this meshpoint</td>
<td>page 27-11</td>
</tr>
<tr>
<td>meshid</td>
<td>Configures a unique ID for this meshpoint</td>
<td>page 27-12</td>
</tr>
<tr>
<td>neighbor</td>
<td>Configures the neighbor inactivity time out for this meshpoint</td>
<td>page 27-13</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 27-14</td>
</tr>
<tr>
<td>root</td>
<td>Configures a meshpoint as the root meshpoint</td>
<td>page 27-17</td>
</tr>
<tr>
<td>security-mode</td>
<td>Configures the security mode on the meshpoint.</td>
<td>page 27-18</td>
</tr>
<tr>
<td>service</td>
<td>Allows only 802.11n capable neighbors to create a mesh connection</td>
<td>page 27-19</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the meshpoint</td>
<td>page 27-20</td>
</tr>
<tr>
<td>use</td>
<td>Configures a QoS policy for use with this meshpoint</td>
<td>page 27-21</td>
</tr>
<tr>
<td>wpa2</td>
<td>Configures WPA2 encryption settings</td>
<td>page 27-22</td>
</tr>
</tbody>
</table>
27.1.1 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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>]**

<table>
<thead>
<tr>
<th>allowed-vlans</th>
<th>Defines VLANs allowed access on the mesh network</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VLAN-ID&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>add &lt;VLAN&gt;</td>
<td>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).</td>
</tr>
<tr>
<td>remove &lt;VLAN&gt;</td>
<td>Removes a single VLAN or a range of VLANs from the list of allowed VLANs.</td>
</tr>
</tbody>
</table>

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
rfs7000-37FABE(config-meshpoint-test)#
```

Related Commands

- **no** Clears the list of VLANs allowed access to the mesh network
27.1.2 beacon-format

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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX5000, NX5240, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
beacon-format [access-point|mesh-point]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>beacon-format</td>
<td>Configures how a mesh capable AP71XX acts in a mesh network</td>
</tr>
<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

```bash
rfs7000-37FABE(config-meshpoint-test)#beacon-format mesh-point
rfs7000-37FABE(config-meshpoint-test)#show context
devices
devices
meshpoint test
meshid test
beacon-format mesh-point
control-vlan 1
allowedvlans 1,10-16,18-23
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>no</td>
<td>Resets the beacon format for this meshpoint to its default (mesh-point)</td>
</tr>
</tbody>
</table>
## 27.1.3 control-vlan

Mesh management traffic can be sent over a dedicated VLAN. This dedicated VLAN is known as a control VLAN. This command configures a VLAN as the dedicated control VLAN.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

### Syntax

```
control-vlan <1-4094>
```

### Parameters

- **control-vlan <1-4094>**

<table>
<thead>
<tr>
<th>control-vlan</th>
<th>The VLAN used as the control VLAN. The default is VLAN 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4094&gt;</td>
<td>Configures a VLAN as a dedicated carrier of mesh management traffic</td>
</tr>
</tbody>
</table>

### 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

- **no**
  - Resets the control VLAN for this meshpoint to its default of 1
27.1.4 data-rates

meshpoint-config-instance

Configures individual data rates for the 2.4 GHz and 5.0 GHz frequency bands

Supported in the following platforms:
- Access Points — AP6522, AP6531, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS8000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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|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|mcs8-15|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|mcs0-7)

<table>
<thead>
<tr>
<th>data-rates 2.4GHz</th>
<th>Configures the preset data rates for the 2.4 GHz frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.</td>
<td></td>
</tr>
</tbody>
</table>
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)

<table>
<thead>
<tr>
<th>Configures custom rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Configures the available rate at 1 Mbps</td>
</tr>
<tr>
<td>2 – Configures the available rate at 2 Mbps</td>
</tr>
<tr>
<td>5.5 – Configures the available rate at 5.5 Mbps</td>
</tr>
<tr>
<td>6 – Configures the available rate at 6 Mbps</td>
</tr>
<tr>
<td>9 – Configures the available rate at 9 Mbps</td>
</tr>
<tr>
<td>11 – Configures the available rate at 11 Mbps</td>
</tr>
<tr>
<td>12 – Configures the available rate at 12 Mbps</td>
</tr>
<tr>
<td>18 – Configures the available rate at 18 Mbps</td>
</tr>
<tr>
<td>24 – Configures the available rate at 24 Mbps</td>
</tr>
<tr>
<td>36 – Configures the available rate at 36 Mbps</td>
</tr>
<tr>
<td>48 – Configures the available rate at 48 Mbps</td>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<td>msc8-15 – 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

- **data-rates 5GHz [a-only|an|default]**

<table>
<thead>
<tr>
<th>data-rates 5GHz</th>
<th>Configures the preset data rates for the 5.0 GHz frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-only</td>
<td>Configures the data rate for the meshpoint using 802.11a only rates</td>
</tr>
<tr>
<td>bn</td>
<td>Configures the data rate for the meshpoint using 802.11a and 802.11n rates</td>
</tr>
<tr>
<td>default</td>
<td>Configures the data rate for the meshpoint at a pre-configured default rate for this frequency</td>
</tr>
<tr>
<td>g-only</td>
<td>Configures the data rate for the meshpoint using 802.11g only rates</td>
</tr>
<tr>
<td>gn</td>
<td>Configures the data rate for the meshpoint using 802.11g and 802.11n rates</td>
</tr>
</tbody>
</table>
- **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)

<table>
<thead>
<tr>
<th>data-rates 5GHz</th>
<th>Configures the preset data rates for the 5.0 GHz frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.</td>
<td></td>
</tr>
</tbody>
</table>

| 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 |
|-----------------|----------------------------------------------------------|
| 6 – Configures the available rate at 6 Mbps |
| 9 – Configures the available rate at 9 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 |
| msc8-15 – Configures the MCS index range of 8-15 as the data rate |

**Note:** Multiple choices can be made from the above list of rates.
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

| no       | Resets data rates for each frequency band for this meshpoint |
27.1.5 description

This command 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

description <DESCRIPTION>

Parameters

- description <DESCRIPTION>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>description</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
### 27.1.6 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

#### Syntax

```
meshid <MESH-SSID>
```

#### Parameters

- `meshid <MESH-SSID>`

<table>
<thead>
<tr>
<th>meshid</th>
<th>Configures a unique SSID for the meshpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MESH-SSID&gt;</td>
<td>The unique SSID configured for this meshpoint</td>
</tr>
</tbody>
</table>

**Note:** The mesh SSID is case sensitive and should not exceed 32 characters.

#### Examples

```
rfs7000-37FABE(config-meshpoint-test)#meshid TestingMeshPoint
rfs7000-37FABE(config-meshpoint-test)#show context
  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
27.1.7 neighbor

This command configures the inactivity time out 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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 time out value for this meshpoint
## 27.1.8 no

Negates meshpoint commands or resets their values to default

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```plaintext
no [allowed-vlans|beacon-format|control-vlan|description|meshid|root|security-mode|shutdown]
no data-rates [2.4GHz|5GHz]
no neighbor inactivity-timeout
no use meshpoint-qos-policy
no wpa2 [key-rotation|psk]
no wpa2 key-rotation [broadcast|unicast]
no wpa2 psk
no service allow-ht-only
```

**Parameters**

- no [allowed-vlans|beacon-format|control-vlan|description|meshid|root|security-mode|shutdown]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no allowed-vlans</td>
<td>Removes all VLANs from the allowed VLANs list</td>
</tr>
<tr>
<td>no beacon-format</td>
<td>Resets the beacon format on this meshpoint to its default of meshpoint</td>
</tr>
<tr>
<td>no control-vlan</td>
<td>Removes the configured control VLAN</td>
</tr>
<tr>
<td>no description</td>
<td>Removes the defined description for this meshpoint</td>
</tr>
<tr>
<td>no meshid</td>
<td>Removes the configured mesh id for this meshpoint</td>
</tr>
<tr>
<td>no root</td>
<td>Removes the configuration of this meshpoint as a root meshpoint</td>
</tr>
<tr>
<td>no security-mode</td>
<td>Removes the configuration of security mode to use on this meshpoint to its default of “none”</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Enables the use of this meshpoint</td>
</tr>
</tbody>
</table>

- no data-rates [2.4GHz|5GHz]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no data-rates</td>
<td>Resets data rate configuration to its default</td>
</tr>
<tr>
<td>2.4GHz</td>
<td>Resets data rate configuration for the 2.4 GHz radio</td>
</tr>
<tr>
<td>5GHz</td>
<td>Resets data rate configuration for the 5.0 GHz radio</td>
</tr>
</tbody>
</table>

- no neighbor inactivity-timeout

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no neighbor</td>
<td>Resets the neighbor related configuration</td>
</tr>
<tr>
<td>inactivity-timeout</td>
<td>Resets the inactivity timeout to its default</td>
</tr>
</tbody>
</table>
- no use meshpoint-qos-policy

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no use meshpoint-qos-policy</td>
<td>Resets the mesh-qos-policy to default mesh-qos-policy</td>
</tr>
</tbody>
</table>

- no wpa2 key-rotation [broadcast|unicast]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no wpa2 key-rotation</td>
<td>Resets the WPA2 encryption key rotation configuration for this meshpoint</td>
</tr>
<tr>
<td>broadcast</td>
<td>Resets the WPA2 key rotation configured for broadcast packets to its default</td>
</tr>
<tr>
<td>unicast</td>
<td>Resets the WPA2 key rotation configured for unicast packets to its default</td>
</tr>
</tbody>
</table>

- no wpa2 psk

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no wpa2 psk</td>
<td>Removes the pre shared key configured for the meshpoint</td>
</tr>
</tbody>
</table>

- no service allow-ht-only

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no wpa2 psk</td>
<td>Removes the restriction that only 802.11n capable neighbor devices can associate with this meshpoint</td>
</tr>
</tbody>
</table>

Examples

```
rfs7000-37FABE(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
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 testcompany
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)#
```

```
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 testcompany
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
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 testcompany
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
no root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowed-vlans</td>
<td>Configures the VLANs allowed on the meshpoint</td>
</tr>
<tr>
<td>beacon-format</td>
<td>Configures the beacon format for the meshpoint AP</td>
</tr>
<tr>
<td>control-vlan</td>
<td>Configures the VLAN on which meshpoint control traffic traverses</td>
</tr>
<tr>
<td>data-rates</td>
<td>Configures the data rates supported per frequency band</td>
</tr>
<tr>
<td>description</td>
<td>Configures a human friendly description for this meshpoint</td>
</tr>
<tr>
<td>meshid</td>
<td>Configures a unique ID for this meshpoint</td>
</tr>
<tr>
<td>neighbor</td>
<td>Configures the neighbor inactivity time out for this meshpoint</td>
</tr>
<tr>
<td>root</td>
<td>Configures a meshpoint as the root meshpoint</td>
</tr>
<tr>
<td>security-mode</td>
<td>Configures the security mode to use on the meshpoint</td>
</tr>
<tr>
<td>service</td>
<td>Allows only 802.11n capable neighbors to create a mesh connection</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the meshpoint</td>
</tr>
<tr>
<td>use</td>
<td>Configures using a QoS policy along with this meshpoint</td>
</tr>
<tr>
<td>wpa2</td>
<td>Configures WPA2 encryption settings</td>
</tr>
</tbody>
</table>
27.1.9 root

meshpoint-config-instance

Configures this meshpoint as the root meshpoint. Root meshpoints are generally tied to an Ethernet backhaul for wired connectivity.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

root

Parameters

None

Examples

rfs7000-37FABE(config-meshpoint-test)#root

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
root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands

no

Removes the configuration of this meshpoint as a root meshpoint
27.1.10 *security-mode*

*meshpoint-config-instance*

Configures the security mode for this meshpoint

Supported in the following platforms:
- Access Points (as root APs only) — AP650, AP622
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Wireless Controllers — RFS8000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
security-mode [none|psk]
```

**Parameters**

- `security-mode [none|psk]`

<table>
<thead>
<tr>
<th>security-mode</th>
<th>Configures the security mode for this meshpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No security is configured for this meshpoint</td>
</tr>
<tr>
<td>psk</td>
<td>Uses <em>Pre Shared Key</em> (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**

```
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
rfs7000-37FABE(config-meshpoint-test)#
```

**Related Commands**

```
no
```

Resets the security configuration for this meshpoint to “none”. This indicates that no security is configured for this meshpoint.
27.1.11 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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"
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 testcompany
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
27.1.12 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax
shutdown

Parameters
None

Examples
rfs7000-37FABE(config-meshpoint-test)#shutdown
rfs7000-37FABE(config)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Enables an AP as a meshpoint</td>
</tr>
</tbody>
</table>
27.1.13 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

Syntax

```
use meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

Parameters

- `use meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>`

<table>
<thead>
<tr>
<th>use meshpoint-qos-policy</th>
<th>Configures this meshpoint to use a predefined meshpoint QoS policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MESHPOINT-QOS-POLICY-NAME&gt;</td>
<td>Defines the meshpoint QoS policy to use with this meshpoint</td>
</tr>
</tbody>
</table>

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"
description 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

- `no` Removes the meshpoint QoS policy associated with this meshpoint
- `meshpoint-qos-policy-config-instance` Creates and configures a meshpoint QoS policy
## 27.1.14 wpa2

This command sets the pre-shared keys and key rotation duration.

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

### Syntax

```
wpa2 [psk|key-rotation]
```

```
wpa2 key-rotation [broadcast|unicast] <30-86400>
```

```
wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]
```

### 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>Configures key rotation interval for broadcast packets</td>
</tr>
<tr>
<td></td>
<td>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 packets</td>
</tr>
<tr>
<td>&lt;30-86400&gt;</td>
<td>Configures key rotation interval from 30 - 86400 seconds for unicast or broadcast transmission</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>2 &lt;SECRET&gt;</td>
</tr>
<tr>
<td></td>
<td>- 0 &lt;SECRET&gt; – Configures a clear text secret</td>
</tr>
<tr>
<td></td>
<td>- 2 &lt;SECRET&gt; – Configures an encrypted secret</td>
</tr>
<tr>
<td></td>
<td>- &lt;SECRET&gt; – Specify the secret key. The shared key should not exceed 127 characters.</td>
</tr>
</tbody>
</table>
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 testcompany
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 testcompany
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
root
rfs7000-37FABE(config-meshpoint-test)#

Related Commands

| no | Resets PSK configuration and key rotation duration |
27.2 meshpoint-qos-policy-config-instance

Mesh Quality of Service (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)#
```

```
rfs7000-37FABE(config-meshpoint-qos-test)#?
```

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-test)#
```

Table 27.2 summarizes the mespoint-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 27-25</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or reverts settings to their default</td>
<td>page 27-27</td>
</tr>
<tr>
<td>rate-limit</td>
<td>Configures the rate limits for this QoS policy</td>
<td>page 27-29</td>
</tr>
</tbody>
</table>
### 27.2.1 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, 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]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Configures the accelerated multicast stream address and forwarding QoS classification</td>
</tr>
<tr>
<td>&lt;MULTICAST-IP&gt;</td>
<td>Specify a list of multicast addresses and classifications. Packets are accelerated when the destination address matches.</td>
</tr>
<tr>
<td>autodetect</td>
<td>Lets the system to automatically detect multicast streams to be accelerated</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>classification</td>
<td>Optional. Defines the QoS classification to apply to a multicast stream. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>• background</td>
</tr>
<tr>
<td></td>
<td>• best effort</td>
</tr>
<tr>
<td></td>
<td>• trust</td>
</tr>
<tr>
<td></td>
<td>• video</td>
</tr>
<tr>
<td></td>
<td>• voice</td>
</tr>
</tbody>
</table>
Examples

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets accelerated multicast configurations for this meshpoint QoS policy</td>
</tr>
</tbody>
</table>
27.2.2 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
no [accelerated-multicast|rate-limit]
```

```
no accelerated-multicast [<MULTICAST-IP>|autodetect]
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 accelerated-multicast [<MULTICAST-IP>|autodetect]**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated-multicast</td>
<td>Resets the accelerated multicast stream address and forwarding QoS classification.</td>
</tr>
<tr>
<td><code>&lt;MULTICAST-IP&gt;</code></td>
<td>Defines the IP address of the multicast stream to be reset.</td>
</tr>
<tr>
<td>autodetect</td>
<td>Lets the system automatically detect multicast streams to be reset.</td>
</tr>
</tbody>
</table>

- **no rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size|rate}**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint</td>
<td>Resets rate limit parameters for a meshpoint.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Resets rate limit parameters for neighboring meshpoint devices.</td>
</tr>
<tr>
<td>from-air</td>
<td>Resets rate limit value for traffic from the wireless neighbor to the network.</td>
</tr>
<tr>
<td>to-air</td>
<td>Resets the rate limit value for traffic from the network to the wireless neighbor.</td>
</tr>
<tr>
<td>max-burst-size</td>
<td>Optional. Resets the maximum burst size in kilobytes.</td>
</tr>
<tr>
<td>rate</td>
<td>Optional. Configures the maximum traffic rate in kilobytes.</td>
</tr>
</tbody>
</table>

- **no rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background|
  best-effort|video|voice]}**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint</td>
<td>Resets rate limit parameters for a meshpoint.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Resets rate limit parameters for neighboring meshpoint devices.</td>
</tr>
<tr>
<td>from-air</td>
<td>Resets the rate limit value for traffic from the wireless neighbor to the network.</td>
</tr>
<tr>
<td>to-air</td>
<td>Resets the rate limit value for traffic from the network to the wireless neighbor.</td>
</tr>
<tr>
<td>red-threshold</td>
<td>Optional. Resets the <em>random early detection</em> (RED) threshold for traffic class. The options are:</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>background</td>
<td>Resets the threshold for low priority traffic</td>
</tr>
<tr>
<td>best-effort</td>
<td>Resets the threshold for best effort traffic</td>
</tr>
<tr>
<td>video</td>
<td>Resets the threshold for video traffic</td>
</tr>
<tr>
<td>voice</td>
<td>Resets the threshold for voice traffic</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
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
rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-threshold
rfs7000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-threshold
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)#
```
27.2.3 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, 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622
- Wireless Controllers — RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500, NX9510, 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>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>max-burst-size &lt;2-1024&gt;</code></td>
<td>Optional. Configures the maximum burst size in kilobytes. Set a value from 2 - 1024 kbytes. 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. 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.</td>
</tr>
<tr>
<td><code>rate &lt;50-1000000&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>meshpoint</code></td>
<td>Configures rate limit parameters for a meshpoint</td>
</tr>
<tr>
<td><code>neighbor</code></td>
<td>Configures rate limit parameters for neighboring meshpoint devices</td>
</tr>
<tr>
<td><code>from-air</code></td>
<td>Configures rate limits for traffic from the wireless neighbor to the network</td>
</tr>
<tr>
<td><code>to-air</code></td>
<td>Configures rate limit value for traffic from the network to the wireless neighbor</td>
</tr>
<tr>
<td><code>red-threshold</code></td>
<td>Optional. Configures <em>random early detection</em> threshold (RED threshold) for traffic class</td>
</tr>
<tr>
<td><code>background &lt;0-100&gt;</code></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>-------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>video &lt;0-100&gt;</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>voice &lt;0-100&gt;</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

```
rsf7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air max-burst-size 800
rsf7000-37FABE(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
rsf7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air rate 80000
rsf7000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-threshold video 80
rsf7000-37FABE(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
rfs7000-37FABE(config-meshpoint-qos-test)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Resets traffic rate limit settings for this meshpoint QoS policy</td>
</tr>
</tbody>
</table>
27.3 meshpoint-device-config-instance

Table 27.3 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 27-34</td>
</tr>
<tr>
<td>meshpoint-device-commands</td>
<td>Invokes the meshpoint-device configuration commands</td>
<td>page 27-36</td>
</tr>
</tbody>
</table>
27.3.1 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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax

meshpoint-device <MESHPOINT-NAME>

Parameters

- meshpoint-device <MESHPOINT-NAME>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>meshpoint-device</td>
<td>Configures the AP as a meshpoint device and sets its parameters</td>
</tr>
<tr>
<td>&lt;MESHPOINT-NAME&gt;</td>
<td>The meshpoint to configure the AP with</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
- 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
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
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

ap731-11B6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#?
### 27.3.2 meshpoint-device-commands

> meshpoint-device-config-instance

Table 27.4 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 27-37</td>
</tr>
<tr>
<td>exclude</td>
<td>Excludes neighboring mesh devices</td>
<td>page 27-41</td>
</tr>
<tr>
<td>hysteresis</td>
<td>Configures path selection SNR hysteresis values on this meshpoint-device (access point)</td>
<td>page 27-42</td>
</tr>
<tr>
<td>monitor</td>
<td>Enables monitoring of critical resource and primary port links on a meshpoint device</td>
<td>page 27-44</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 27-45</td>
</tr>
<tr>
<td>preferred</td>
<td>Configures the preferred path parameters for a meshpoint device</td>
<td>page 27-46</td>
</tr>
<tr>
<td>root</td>
<td>Configures a meshpoint device as the root meshpoint</td>
<td>page 27-47</td>
</tr>
<tr>
<td>root-select</td>
<td>Configures this meshpoint device as the cost root</td>
<td>page 27-49</td>
</tr>
<tr>
<td>no</td>
<td>Negates the commands for a meshpoint device or resets values to default</td>
<td>page 27-50</td>
</tr>
</tbody>
</table>
27.3.2.1 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, AP7502, AP7522, AP7532, 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|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|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 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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-hold-time [2.4GHz</td>
<td>5GHz] &lt;0-86400&gt;</td>
</tr>
</tbody>
</table>
  - 2.4 GHz – Configures the channel hold interval for the 2.4 GHz radio band
  - 5.0 GHz – Configures the channel hold interval for the 5.0 GHz radio band
| Note: | A value of ‘0’ disables periodic channel assessment. |
### `acs channel-switch-delta [2.4GHz|5GHz] <5-35>`

|acs channel-switch-delta [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. |
|---|---|
|2.4 GHz – Configures the channel switch delta for the 2.4GHz radio band |
|5.0GHz – Configures the channel switch delta for the 5.0 GHz radio band |
|The following keyword is common to the ‘2.4 GHz’ and ‘5.0 GHz’ bands: |
|<5-35> – Specify a value from 5 - 35 dBm. The default is 10 dBm. |

### `acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|auto]`

|acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|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 |
|auto – Selects and assigns the best possible channel from the 20/40 MHz width. This is the default setting. |

### `acs ocs-duration [2.4GHz|5GHz] <20-250>`

|acs ocs-duration [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. |

### `acs ocs-frequency [2.4GHz|5GHz] <1-60>`

<p>|acs ocs-frequency [2.4GHz|5GHz] &lt;1-60&gt; | 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: |
|&lt;1-60&gt; – Specify a value form 1 - 60 seconds. The default is 6 seconds. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acs path-min [2.4GHz</td>
<td>5GHz] &lt;100-20000&gt;</td>
</tr>
<tr>
<td></td>
<td>• 2.4 GHz – Configures the minimum root path metric for the 2.4 GHz radio band&lt;br&gt;• 5.0 GHz – Configures the minimum root path metric for the 5.0 GHz radio band&lt;br&gt;The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:&lt;br&gt;• &lt;100-20000&gt; – Specify a value from 100 - 20000. The default is 1000.</td>
</tr>
<tr>
<td>acs path-threshold [2.4GHz</td>
<td>5GHz] &lt;800-65535&gt;</td>
</tr>
<tr>
<td></td>
<td>• 2.4 GHz – Configures the root path metric threshold for the 2.4 GHz radio band&lt;br&gt;• 5.0 GHz – Configures the root path metric threshold for the 5.0 GHz radio band&lt;br&gt;The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:&lt;br&gt;• &lt;800-65535&gt; – Specify a value from 800 -65535. The default is 1500.</td>
</tr>
<tr>
<td>acs priority-meshpoint [2.4GHz</td>
<td>5GHz] &lt;MESHPOINT-NAME&gt;</td>
</tr>
<tr>
<td>acs sample-count [2.4GHz</td>
<td>5GHz] &lt;1-10&gt;</td>
</tr>
<tr>
<td>acs snr-delta [2.4GHz</td>
<td>5GHz] &lt;1-100&gt;</td>
</tr>
</tbody>
</table>
### 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 [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 [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

```bash
rfs4000-229D58 (config-profile-testAP71XX-meshpoint-test)#acs channel-hold-time 2.4GHz 2500
rfs4000-229D58 (config-profile-testAP71XX-meshpoint-test)#
rfs4000-229D58 (config-profile-testAP71XX-meshpoint-test)#acs ocs-duration 2.4GHz 30
rfs4000-229D58 (config-profile-testAP71XX-meshpoint-test)#
rfs4000-229D58 (config-profile-testAP71XX-meshpoint-test)#acs ocs-frequency 2.4GHz 1
rfs4000-229D58 (config-profile-testAP71XX-meshpoint-test)#
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

- **no**

  Reverts the configured ACS settings to default
27.3.2.2 **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, AP7502, AP7522, AP7532, 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 MiNT level-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)#
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
27.3.2.3 **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, AP7502, AP7522, AP7532, 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**

- `hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-100>|snr-delta <1-100>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 min-threshold -65
  hysteresis root-sel-snr-delta 12
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>Removes the configured path selection SNR hysteresis values</td>
</tr>
</tbody>
</table>
27.3.2.4 **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, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622

**Syntax**

```plaintext
monitor [critical-resource|primary-port-link-loss]
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</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.
27.3.2.5 path-method

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, AP7502, AP7522, AP7532, 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 connections 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. <strong>Note:</strong> 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. <strong>Note:</strong> 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)#

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 |
27.3.2.6 prefered

meshpoint-device-commands

Configures the preferred path parameters for this meshpoint device

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, 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]]

  | preferred | Configures the preferred path parameters |
  | neighbor <MAC> | Adds the MAC address of a neighbor meshpoint as a preferred neighbor |
  | root <MAC> | Adds the MAC address of a root meshpoint as a preferred root |
  | interface [2.4GHz|4.9GHz|5GHz] | Sets the preferred interface |

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
27.3.2.7 root

meshpoint-device-commands

Configures 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, AP7502, AP7522, AP7532, 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>root</th>
<th>Configures this meshpoint device as the root meshpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>select-method auto-mint</td>
<td>Optional. Enables or disables dynamic mesh selection. When enabled, this option overrides root or no-root configuration and chooses the selection method.</td>
</tr>
<tr>
<td></td>
<td>• auto-mint — Enables dynamic root selection using Auto-MiNT (based on path cost)</td>
</tr>
<tr>
<td></td>
<td>Note: The Auto-Mint or Cost Method dynamically determines the root/non-root configuration of a meshpoint by:</td>
</tr>
<tr>
<td></td>
<td>• Monitoring and ranking the signal strength and path cost of neighboring mesh points.</td>
</tr>
<tr>
<td></td>
<td>• Setting the configuration to:</td>
</tr>
<tr>
<td></td>
<td>• non-root: If the link with the shortest path to the cost-root mesh device is a MCX mesh-point link</td>
</tr>
<tr>
<td></td>
<td>• root: If the link with the shortest path to the cost-root mesh device is a non MCX mesh-point link (wired link).</td>
</tr>
<tr>
<td></td>
<td>• 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 &gt; cost-root command to configure a meshpoint-device as ‘cost-root’.</td>
</tr>
<tr>
<td></td>
<td>• Using signal strength of neighboring meshpoint as the sole metric to determine the next mesh hop to the root.</td>
</tr>
<tr>
<td></td>
<td>• Loop detection with both meshpoints in a car select non-root and form a mesh link with the same root</td>
</tr>
<tr>
<td></td>
<td>• auto-proximity — 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>

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)#
```
apt131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root select-method auto-mint
apt131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context meshpoint-device test
   root select-method auto-mint
apt131-11E6C4(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>
27.3.2.8 root-select

Configures this meshpoint device as the cost root

Supported in the following platforms:
- Access Points — AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP8132
- Access Points (as root APs only) — AP650, AP622

Syntax

root-select cost-root

Parameters

- root-select cost-root

<table>
<thead>
<tr>
<th>root-select cost-root</th>
<th>Configures this meshpoint device as the cost root. This is necessary for dynamic root selection process. Select this option to set the meshpoint as the cost root for meshpoint root selection. This setting is disabled by default.</th>
</tr>
</thead>
</table>

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
  meshpoint-device test
  root select-method auto-mint
  root-select cost-root

Related Commands

no | Removes this meshpoint-device as the cost-root |
27.3.2.9 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, AP7502, AP7522, AP7532, 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|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 acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|
ocs-frequency|path-min|path-threshold|priority-meshpoint|sample-count|snr-delta|
signal-threshold|tolerance-period] [2.4GHZ|5GHz]

no acs
channel-hold-time Reverts the automatic channel selection settings to default
channel-switch-delta Reverts channel hold time to default (1800 seconds)
channel-width Reverts channel switch delta to default (10 dBm)
channel-width Reverts channel width to default (auto)
ocsc-duration Reverts off -channel scan duration to default (50 milliseconds)
ocsc-frequency Reverts off -channel scan frequency to default (6 seconds)
path-min Reverts the minimum root path metric to default (1000)
path-threshold Reverts the root path metric threshold to default (1500)
priority-meshpoint Disables the priority meshpoint configuration
sample-count Reverts the sample count to default (5 samples)
snr-delta Reverts the channel SNR delta to default (5 db)
signal-threshold Reverts the signal strength threshold to default (-65 dB)
tolerance-period Reverts the tolerance period to default (60 seconds)

- no exclude wired-peer mint-level-1

no exclude wired-peer Disables exclusion of wired peers (wired mesh devices) with MiNT level-1 link
• no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]

| no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta] | Removes the configured path selection SNR hysteresis values |

• no monitor [critical-resource|primary-port-link-loss]

| no monitor critical-resource | Disables critical resource down event monitoring |
| no monitor primary-port-link-loss | Disables primary port link loss event monitoring |

• no [path-method|root {select-method}]

| no root select-method | Removes the configuration of this meshpoint device as a root meshpoint. Also allows you to disable dynamic mesh selection (if enabled). |
| no path-method | Resets the path selection method (path to the root node) to default (uniform) |

• no root-select cost-root

| no root-select cost-root | Removes the selected meshpoint-device as the cost-root |

• no preferred [interface|root|neighbor]

| no preferred | Resets the preferred path configuration |
| interface | Resets the preferred interface |
| root | Resets the preferred root to none |
| neighbor | Resets the preferred neighbor to none |

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.

WiNG 5.5.6 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:

```plaintext
<DEVICE>(config)#passpoint-policy <POLICY-NAME>
```

```
rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#
```

```
rfs4000-229D58(config-passpoint-policy-test)#?
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
    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)#
```
## 28.1 passpoint-policy

Table 28.1 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 28-4</td>
</tr>
<tr>
<td>access-network-type</td>
<td>Configures the access network type element in this hotspot</td>
<td>page 28-5</td>
</tr>
<tr>
<td>connection-captability</td>
<td>Configures the connection capability element in this passpoint policy</td>
<td>page 28-6</td>
</tr>
<tr>
<td>domain-name</td>
<td>Configures the RF Domains to which this hotspot is applicable</td>
<td>page 28-8</td>
</tr>
<tr>
<td>hessid</td>
<td>Configures the Homogeneous Extended Service Set Identifier (HESSID) for a specified hotspot zone</td>
<td>page 28-9</td>
</tr>
<tr>
<td>internet</td>
<td>Advertises the availability of Internet access in this hotspot</td>
<td>page 28-10</td>
</tr>
<tr>
<td>ip-address-type</td>
<td>Advertises the IP address type used in this hotspot.</td>
<td>page 28-11</td>
</tr>
<tr>
<td>nai-realm</td>
<td>Configures a Network Access Identifier (NAI) realm name and enters its configuration mode</td>
<td>page 28-13</td>
</tr>
<tr>
<td>net-auth-type</td>
<td>Configures the network authentication type used in this hotspot</td>
<td>page 28-19</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts passpoint policy configuration</td>
<td>page 28-20</td>
</tr>
<tr>
<td>operator</td>
<td>Configures the operator friendly name for this hotspot</td>
<td>page 28-22</td>
</tr>
<tr>
<td>roam-consortium</td>
<td>Configures the list of Roaming Consortium Organization Identifiers (OIs) supported on this hotspot</td>
<td>page 28-23</td>
</tr>
<tr>
<td>venue</td>
<td>Configures the venue group and type for this passpoint policy</td>
<td>page 28-24</td>
</tr>
<tr>
<td>wan-metrics</td>
<td>Configures the WAN performance metrics for this hotspot</td>
<td>page 28-28</td>
</tr>
</tbody>
</table>
28.1.1 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, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

Syntax

3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}

Parameters

- 3gpp <1-20> mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>Configures the 3GPP PLMN information that is returned in response to an ANQP query</td>
</tr>
<tr>
<td>mcc &lt;MOBILE-COUNTRY-CODE&gt;</td>
<td>Specifies the MCC. The MCC is a two or three digit decimal value. For example, the MCC for Australia is 505.</td>
</tr>
<tr>
<td>mnc &lt;MOBILE-NETWORK-CODE&gt;</td>
<td>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). <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>description &lt;LINE&gt;</td>
<td>Optional. Configures a description that uniquely identifies this PLMN. Provide a description not exceeding 64 characters in length.</td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#

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 |
### 28.1.2 access-network-type

*passpoint-policy*

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, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

**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.

```plaintext
rfs4000-229D58(config-passpoint-policy-test)#access-network-type chargeable-public
rfs4000-229D58(config-passpoint-policy-test)#
```

**Examples**

```plaintext
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)
### 28.1.3 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, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

**Syntax**

```
connection-capability [ftp|http|icmp|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]
connection-capability [ftp|http|icmp|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|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn] [closed|open|unknown]`
  - `connection-capability` Configures the connection capability element in this passpoint policy
  - `ftp` Specifies the protocol type as FTP. Configures TCP port 20.
  - `http` Specifies the protocol type as HTTP. Configures TCP port 80.
  - `icmp` Specifies the protocol type as ICMP.
  - `ipsec-vpn` Specifies the protocol type as IPSEC VPN. Configures ESP and UDP ports 500 and 4500.
  - `pptp-vpn` Specifies the protocol type as PPTP VPN. Configures TCP port 1723.
  - `sip` Specifies the protocol type as SIP. Configures TCP port 5060 and UDP port 5060.
  - `ssh` Specifies the protocol type as SSH. Configures TCP port 20
  - `tls-vpn` Specifies the protocol type as TLS VPN. Configures TCP port 443.
  - `port <0-65535> [closed|open|unknown]`
    - After specifying the protocol type, specify the port (associated with the selected protocol) and its status.
      - `closed` – Specifies that the port(s) is/are closed
      - `open` – Specifies that the port(s) is/are open
      - `unknown` – Specifies that the port(s) status is not known
  - **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]
```

- `connection-capability` Configures the connection capability element in this passpoint policy
- `ip-protocol <0-255>` Identifies the IP protocol by the protocol’s number. For example, for *simple message protocol* (SMP) specify 121.
### Examples

```
rfs4000-229D58(config-passpoint-policy-test)#connection-capability 1 ip-protocol 2 port 10 closed
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
  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>
28.1.4 domain-name

Configure the RF Domain(s) that 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, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

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)#
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
28.1.5 **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 behaviour. 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, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

**Syntax**

```
hessid <MAC>
```

**Parameters**

- `hessid <MAC>`

<table>
<thead>
<tr>
<th>hessid &lt;MAC&gt;</th>
<th>Specify a unique 6 (six) byte identifier for this passpoint policy.</th>
</tr>
</thead>
</table>

**Examples**

```
rfs4000-229D58(config-passpoint-policy-test)#hessid 00-23-68-88-0D-A7
rfs4000-229D58(config-passpoint-policy-test)#
```

```
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot-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.
28.1.6 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, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

Syntax
internet

Parameters
None

Examples
rfs4000-229D58(config-passpoint-policy-test)#internet
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

| no | Removes Internet access on this passpoint policy |
### 28.1.7 ip-address-type

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 — AP300, AP621, AP622, AP650, ES6510, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, NX6500, NX6524, NX9000, NX9500, NX9510

**Syntax**

```
ip-address-type [ipv4|ipv6]
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 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 ipv6** [available|not-available|unknown]

<table>
<thead>
<tr>
<th>ip-address-type ipv4</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>double-nat</td>
<td>Specifies double NATed private IPv4 address is available</td>
</tr>
<tr>
<td>not-available</td>
<td>Specifies IPv4 address is not available</td>
</tr>
<tr>
<td>port-restricted</td>
<td>Specifies port-restricted IPv4 address is available</td>
</tr>
<tr>
<td>port-restricted-double-nat</td>
<td>Specifies port-restricted IPv4 address and double NATed IPv4 address is available</td>
</tr>
<tr>
<td>port-restricted-single-nat</td>
<td>Specifies port-restricted IPv4 address and single NATed IPv4 address is available</td>
</tr>
<tr>
<td>public</td>
<td>Specifies public IPv4 address is available</td>
</tr>
<tr>
<td>single-nat</td>
<td>Specifies single NATed IPv4 address is available</td>
</tr>
<tr>
<td>unknown</td>
<td>Specifies no information configured regarding the IPv4 address availability</td>
</tr>
</tbody>
</table>

- **ip-address-type ipv6** [available|not-available|unknown]

<table>
<thead>
<tr>
<th>ip-address-type ipv6</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>available</td>
<td>Configures IPv6 address type availability information</td>
</tr>
<tr>
<td>not-available</td>
<td>Specifies IPv6 address is not available</td>
</tr>
<tr>
<td>unknown</td>
<td>Specifies no information configured regarding the IPv6 address availability</td>
</tr>
</tbody>
</table>
Examples

rfs4000-229D58(config-passpoint-policy-test)#ip-address-type ipv6 available
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 00-23-68-88-0D-A7
  ip-address-type ipv6 available
    3gpp mcc 310 mnc 970
    3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

Related Commands

| no          | Removes the IP address type configured for this passpoint policy |
28.1.8 nai-realm

A Network Access Identifier (NAI) realm element in the passpoint policy identifies a hotspot service provider by the unique NAI realm name.

Table 28.2 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 28-14</td>
</tr>
<tr>
<td>nai-realm-config-mode commands</td>
<td>Invokes the NAI realm configuration mode commands</td>
<td>page 28-16</td>
</tr>
</tbody>
</table>
28.1.8.1 nai-realm

* 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 hotpsot 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, AP6532, AP6562, AP71XX, AP81XX, AP7502, AP7522, AP7532, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

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.testrealm.com
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.testrealm.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

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#exit
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#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
  nai-realm mail.testrealm.com
  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>no</td>
<td>Removes the NAI realm name configured for this passpoint policy</td>
</tr>
</tbody>
</table>
28.1.8.2 nai-realm-config-mode commands

Table 28.3 summarizes NAI realm configuration 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 Extensible Authentication Protocol (EAP) authentication mechanisms supported by each of the service providers associated with this passpoint policy</td>
<td>page 28-17</td>
</tr>
</tbody>
</table>
28.1.8.2.1 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, AP81XX, AP7502, AP7522, AP7532, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

**Syntax**

eap-method <1-10> [<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|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]

**Parameters**

- **eap-method <1-10> [<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|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]**

<table>
<thead>
<tr>
<th>eap-method &lt;1-10&gt;</th>
<th>Creates an EAP authentication method and assigns it an index number</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-10&gt;</td>
<td>Specify a identifier for this EAP method from 1 - 10.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>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).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;1-255&gt;</th>
<th>Identifies the EAP authentication method type from the corresponding <em>Internet Assigned Numbers Authority</em> (IANA) number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>&lt;1-255&gt; – Specify the IANA identity number for the authentication protocol from 1 - 255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>fast</th>
<th>Specifies the EAP authentication method type as <em>Flexible Authentication via Secure Tunneling</em> (FAST)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtc</td>
<td>Specifies the EAP authentication method type as <em>Generic Token Card</em> (GTC)</td>
</tr>
<tr>
<td>identity</td>
<td>Specifies the EAP authentication method type as Identification</td>
</tr>
<tr>
<td>ikev2</td>
<td>Specifies the EAP authentication method type as <em>Internet Key Exchange Protocol version 2</em> (IKEv2)</td>
</tr>
<tr>
<td>ms-auth</td>
<td>Specifies the EAP authentication method type as <em>Microsoft Authentication</em> (MS-Auth)</td>
</tr>
<tr>
<td>mschapv2</td>
<td>Specifies the EAP authentication method type as <em>Microsoft Challenge Handshake Authentication Protocol version 2</em> (MSCHAPv2)</td>
</tr>
<tr>
<td>opt</td>
<td>Specifies the EAP authentication method type as <em>One Time Password</em> (OTP)</td>
</tr>
<tr>
<td>peap</td>
<td>Specifies the EAP authentication method type as <em>Protected Extensible Authentication Protocol</em> (PEAP)</td>
</tr>
<tr>
<td>psk</td>
<td>Specifies the EAP authentication method type as <em>Pre-shared Key</em> (PSK)</td>
</tr>
<tr>
<td>rsa-public-key</td>
<td>Specifies the EAP authentication method type as RSA public key protocol</td>
</tr>
<tr>
<td>sim</td>
<td>Specifies the EAP authentication method type as <em>GSM Subscriber Identity Module</em> (SIM)</td>
</tr>
<tr>
<td>tls</td>
<td>Specifies the EAP authentication method type as <em>Transport Layer Security</em> (TLS)</td>
</tr>
</tbody>
</table>
Examples
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
ttls auth-param vendor hex 00001E
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-method 2
rsa-public-key auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-method 3
otp auth-param credential username-password
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
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)#
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#show context
nai-realm mail.example.com
eap-method 1 ttls 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)#
```
28.1.9 net-auth-type

Configures 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, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

Syntax

net-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url <URL>}

Parameters

- net-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url <URL>}
- accept-terms Enables user acceptance of terms and conditions
- dns-redirect Enables DNS redirection of user
- http-redirect Enables HTTP redirection of user
- online-enroll Enables online user enrolment
- url <URL> Optional. Specify the location for each of above network authentication types.

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
collection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
hesid 00-23-68-88-0D-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
28.1.10 no

- **passpoint-policy**
  Removes or reverts the passpoint policy settings

Supported in the following platforms:
- Access Points — AP621, AP622, AP650, AP6511, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

**Syntax**

```
no [3gpp|access-network-type|connection-capability|domain-name|hessid|internet|
ip-address-type|nai-realm|net-auth-type|operator|roam-consortium|venue|wan-metrics]
```

**Parameters**
- no [3gpp|access-network-type|connection-capability|domain-name|hessid|internet|
ip-address-type|nai-realm|net-auth-type|operator|roam-consortium|venue|wan-metrics]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no 3gpp</td>
<td>Removes the specified 3GPP PLMN ID and its corresponding MCC/MNC settings</td>
</tr>
<tr>
<td>no access-network-type</td>
<td>Reverts to the default access network type setting (private)</td>
</tr>
<tr>
<td>no connection-capability</td>
<td>Removes the configured connection capability element on the hotspot</td>
</tr>
<tr>
<td>no domain-name</td>
<td>Removes the RF Domain mapped to the hotspot</td>
</tr>
<tr>
<td>no hessid</td>
<td>Removes the HESSID configured on the hotspot and reverts back to using the radio's BSSID</td>
</tr>
<tr>
<td>no internet</td>
<td>Removes Internet access on this hotspot</td>
</tr>
<tr>
<td>no ip-address-type</td>
<td>Removes the IP address type applicable on this hotspot</td>
</tr>
<tr>
<td>no nai-realm</td>
<td>Removes the NAI realm name configured for this hotspot</td>
</tr>
<tr>
<td>no net-auth-type</td>
<td>Removes the network authentication type configured with this hotspot</td>
</tr>
<tr>
<td>no operator</td>
<td>Removes the operator friendly name configured for this hotspot</td>
</tr>
<tr>
<td>no roam-consortium</td>
<td>Removes the Roaming Consortium OIs supported on this hotspot</td>
</tr>
<tr>
<td>no venue</td>
<td>Removes the venue group and type configured with this hotspot</td>
</tr>
<tr>
<td>no wan-metrics</td>
<td>Removes the WAN metrics configuration on this hotspot</td>
</tr>
</tbody>
</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
hotspot-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 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)#

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)#
28.1.11 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, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

Syntax

operator name [ <OPERATOR-NAME>|iso-lang <ISO-LANG-CODE>] 
operator name <OPERATOR-NAME>
operator name iso-lang <ISO-LANG-CODE> <OPERATOR-NAME>

Parameters

- operator name <OPERATOR-NAME>

<table>
<thead>
<tr>
<th>name &lt;OPERATOR-NAME&gt;</th>
<th>Configures the operator's name in English</th>
</tr>
</thead>
<tbody>
<tr>
<td>• &lt;OPERATOR-NAME&gt; — Specify the operator friendly name in ASCII format.</td>
<td></td>
</tr>
</tbody>
</table>

- operator name iso-lang <ISO-LANG-CODE> <OPERATOR-NAME>

<table>
<thead>
<tr>
<th>name iso-lang &lt;ISO-LANG-CODE&gt; &lt;OPERATOR-NAME&gt;</th>
<th>Configures a non-English operator's name</th>
</tr>
</thead>
<tbody>
<tr>
<td>• iso-lang &lt;ISO-LANG-CODE&gt; — Identifies the language by its ISO 639 language code (for example, ‘chi-chinese’ or ‘spa-spanish’).</td>
<td></td>
</tr>
<tr>
<td>• &lt;ISO-LANG-CODE&gt; — Specify the 3 character iso-639 language code (for example, ‘chi-chinese’ or ‘spa-spanish</td>
<td></td>
</tr>
<tr>
<td>• &lt;OPERATOR-NAME&gt; — Specifies the operator’s name as a hexadecimal code</td>
<td></td>
</tr>
</tbody>
</table>

Examples

rfs4000-229D58(config-passpoint-policy-test)#operator name emergencyservices
rfs4000-229D58(config-passpoint-policy-test)#

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-realma тестrealm.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
28.1.12 roam-consortium

Configure 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, AP6521, AP6522, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

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>&lt;WORD&gt;</td>
<td>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)#

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
28.1.13 venue

*passpoint-policy*

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, AP6521, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

**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

<table>
<thead>
<tr>
<th><strong>venue group</strong></th>
<th>Configures the venue group associated with this hotspot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>assembly type</strong></td>
<td>Configures the venue group as assembly (1). This hotspot type is applicable to public assembly venues.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td>&lt;0-255&gt;</td>
<td>Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td>amphitheater</td>
<td>Specifies the venue type as amphitheater (4)</td>
</tr>
<tr>
<td>amusement-park</td>
<td>Specifies the venue type as amusement park (5)</td>
</tr>
<tr>
<td>arena</td>
<td>Specifies the venue type as arena (1)</td>
</tr>
<tr>
<td>bar</td>
<td>Specifies the venue type as bar (12)</td>
</tr>
<tr>
<td>coffee-shop</td>
<td>Specifies the venue type as a coffee shop (13)</td>
</tr>
<tr>
<td>convention-centre</td>
<td>Specifies the venue type as a convention center (7)</td>
</tr>
<tr>
<td>emergency-coordination-center</td>
<td>Specifies the venue type as a emergency coordination center (15)</td>
</tr>
<tr>
<td>library</td>
<td>Specifies the venue type as a library (8)</td>
</tr>
<tr>
<td>museum</td>
<td>Specifies the venue type as a museum (9)</td>
</tr>
<tr>
<td>passenger-terminal</td>
<td>Specifies the venue type as a passenger terminal (3)</td>
</tr>
<tr>
<td>place-of-worship</td>
<td>Specifies the venue type as a place of worship (6)</td>
</tr>
<tr>
<td>restaurant</td>
<td>Specifies the venue type as a restaurant (10)</td>
</tr>
<tr>
<td>stadium</td>
<td>Specifies the venue type as a stadium (2)</td>
</tr>
<tr>
<td>theater</td>
<td>Specifies the venue type as a theater (11)</td>
</tr>
<tr>
<td>unspecified</td>
<td>Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>zoo</td>
<td>Specifies the venue type as a zoo (14)</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>business type</strong></td>
<td>Configures the venue group as business (2). This hotspot type is applicable to business venues.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</td>
</tr>
<tr>
<td></td>
<td>• attorney – Specifies the venue type as the attorney’s office (9)</td>
</tr>
<tr>
<td></td>
<td>• bank – Specifies the venue type as a bank (2)</td>
</tr>
<tr>
<td></td>
<td>• doctor – Specifies the venue type as a doctor or dentist’s office (1)</td>
</tr>
<tr>
<td></td>
<td>• fire-station – Specifies the venue type as a fire station (3)</td>
</tr>
<tr>
<td></td>
<td>• police-station – Specifies the venue type as a police station (4)</td>
</tr>
<tr>
<td></td>
<td>• post-office – Specifies the venue type as a post office (5)</td>
</tr>
<tr>
<td></td>
<td>• professional-office – Specifies the venue type as a professional office (7)</td>
</tr>
<tr>
<td></td>
<td>• research-and-development-facility – Specifies the venue type as a research facility (8)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td><strong>educational</strong></td>
<td>Configures the venue group as educational (3). This hotspot type is applicable to educational institutions.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</td>
</tr>
<tr>
<td></td>
<td>• school-primary – Specifies the venue type as a primary school (1)</td>
</tr>
<tr>
<td></td>
<td>• school-secondary – Specifies the venue type as a secondary school (2)</td>
</tr>
<tr>
<td></td>
<td>• university – Specifies the venue type as a university or college (3)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td><strong>industrial</strong></td>
<td>Configures the venue group as industrial (4). This hotspot type is applicable to industrial venues.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</td>
</tr>
<tr>
<td></td>
<td>• factory – Specifies the venue type as a factory (1)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td><strong>institutional</strong></td>
<td>Configures the venue group as institutional (4). This hotspot type is applicable to public health and other institutions.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</td>
</tr>
<tr>
<td></td>
<td>• group-home – Specifies the venue type as a group-home (4)</td>
</tr>
<tr>
<td></td>
<td>• hospital – Specifies the venue type as a hospital (1)</td>
</tr>
<tr>
<td></td>
<td>• long-term-care – Specifies the venue type as a long term care facility (2)</td>
</tr>
<tr>
<td></td>
<td>• prison – Specifies the venue type as a prison or jail (5)</td>
</tr>
<tr>
<td></td>
<td>• rehab – Specifies the venue type as a rehabilitation facility (3)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td><strong>mercantile</strong></td>
<td>Configures the venue group as mercantile (6). This hotspot type is applicable to public mercantile venues.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</td>
</tr>
<tr>
<td></td>
<td>• automotive – Specifies the venue type as a automotive service center (3)</td>
</tr>
<tr>
<td></td>
<td>• gas-station – Specifies the venue type as a gas station (5)</td>
</tr>
<tr>
<td></td>
<td>• grocery – Specifies the venue type as a grocery store (2)</td>
</tr>
<tr>
<td></td>
<td>• mall – Specifies the venue type as a shopping mall (4)</td>
</tr>
<tr>
<td></td>
<td>• retail – Specifies the venue type as a retail store (1)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>Venue Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>outdoor</td>
<td>Configures the venue group as outdoor (11). This hotspot type is applicable to public outdoor venues.</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td></td>
<td>• bus-stop – Specifies the venue type as a bus stop (5)</td>
</tr>
<tr>
<td></td>
<td>• city-park – Specifies the venue type as a city park (2)</td>
</tr>
<tr>
<td></td>
<td>• kiosk – Specifies the venue type as a kiosk (6)</td>
</tr>
<tr>
<td></td>
<td>• muni-mesh – Specifies the venue type as a muni-mesh (municipal wireless Wi-Fi) (1)</td>
</tr>
<tr>
<td></td>
<td>• rest-area – Specifies the venue type as a rest area (3)</td>
</tr>
<tr>
<td></td>
<td>• traffic-control – Specifies the venue type as a traffic control area (4)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>residential</td>
<td>Configures the venue group as residential (7). This hotspot type is applicable to residential complexes.</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td></td>
<td>• boarding-house – Specifies the venue type as a boarding-house (4)</td>
</tr>
<tr>
<td></td>
<td>• dorm – Specifies the venue type as a dormitory (3)</td>
</tr>
<tr>
<td></td>
<td>• hotel – Specifies the venue type as a hotel or motel (2)</td>
</tr>
<tr>
<td></td>
<td>• private – Specifies the venue type as a private residence (1)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>storage</td>
<td>Configures the venue group as storage (8). This hotspot type is applicable to storage groups.</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>unspecified</td>
<td>Configures the venue group as unspecified (0)</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>utility-and-misc</td>
<td>Configures the venue group as utility and miscellaneous (8)</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
<tr>
<td>vehicular</td>
<td>Configures the venue group as vehicular (7). This hotspot type is applicable to mobile venues.</td>
</tr>
<tr>
<td></td>
<td>• type – Specifies the venue type for this group. The options are:</td>
</tr>
<tr>
<td></td>
<td>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 - 255</td>
</tr>
<tr>
<td></td>
<td>• airplane – Specifies the venue type as an airplane (2)</td>
</tr>
<tr>
<td></td>
<td>• auto – Specifies the venue type as an automobile or truck (1)</td>
</tr>
<tr>
<td></td>
<td>• bus – Specifies the venue type as a bus (3)</td>
</tr>
<tr>
<td></td>
<td>• ferry – Specifies the venue type as a ferry (5)</td>
</tr>
<tr>
<td></td>
<td>• motor-bike – Specifies the venue type as a motor bike (7)</td>
</tr>
<tr>
<td></td>
<td>• ship – Specifies the venue type as a ship or boat (5)</td>
</tr>
<tr>
<td></td>
<td>• train – Specifies the venue type as a train (6)</td>
</tr>
<tr>
<td></td>
<td>• unspecified – Specifies the venue type as not specified (0)</td>
</tr>
</tbody>
</table>
- **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**

```bash
rfs4000-229D58(config-passpoint-policy-test)#venue name PublicSchool
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#venue group assembly type coffee-shop
rfs4000-229D58(config-passpoint-policy-test)#

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.
28.1.14 wan-metrics

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, AP6532, AP6562, AP71XX, AP7502, AP7522, AP7532, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX9000

Syntax
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>

Parameters
- wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>

Examples
rfs4000-229D58(config-passpoint-policy-test)#wan-metrics down-speed 2000 up-speed 2000
rfs4000-229D58(config-passpoint-policy-test)#

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
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
This chapter summarizes the crypto Certificate Management Protocol (CMP) policy commands in the CLI command structure. CMP is a protocol designed to generate and manage device certificates within a managed network. These certificates are needed for authentication and security purposes.

The WiNG software 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 CMP supported certificate authority (CA) server. It also allows the device to download the certificate from the CA server.

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:
cm-server  CMP CA Server configuration commands
cert-update Enable cert renewal of certificate when about to expire
key-update Enable key-update for the installed certificates
no Negate a command or set its defaults
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
29.1 crypto-cmp-policy-instance

Table 29.1 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 29-3</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 29-4</td>
</tr>
<tr>
<td>use</td>
<td>Associates a device's autogen-uniqueid with this crypto CMP policy</td>
<td>page 29-6</td>
</tr>
<tr>
<td>no</td>
<td>Removes the crypto CMP policy settings</td>
<td>page 29-7</td>
</tr>
</tbody>
</table>
29.1.1 **ca-server**

Configure the CA server details. CA server settings are required to complete CMP requests.

A CA is a network authority that generates and issues digital certificates in response to requests received from network devices.

The CA is an external, trusted third-party server. Use this command to configure the CA server details, such as the 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 CA server and retrieve the certificate from the specified location.

Supported in the following platforms:
- Access Points — AP6522, WiMod
- Service Platforms — NX9500, NX9600

**Syntax**

```
ca-server host <IP/HOSTNAME> port <PORT-NUMBER> path <PATH>
```

**Parameters**

- **ca-server host <IP/HOSTNAME> port <PORT-NUMBER> path <PATH>**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca-server</td>
<td>Configures the CA server details</td>
</tr>
<tr>
<td>host &lt;IP/HOSTNAME&gt;</td>
<td>Configures IP address or hostname of the device hosting the CA server.</td>
</tr>
<tr>
<td>port &lt;PORT-NUMBER&gt;</td>
<td>Configures the port on which the CA server can be reached.</td>
</tr>
<tr>
<td>path &lt;PATH&gt;</td>
<td>Configures the path or filename of the CA certificate. Enter the complete relative path to the file on the server.</td>
</tr>
</tbody>
</table>

**Examples**

```
ap6522-D8273A(config-cmp-policy-CMP)#ca-server host 192.168.8.74 port 80 path cmp
```

```
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
cac-server host 192.168.8.74 port 80 path cmp
```

**Related Commands**

- **no** Removes the configured CA server details
29.1.2 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 — AP6522, WiMod
- Service Platforms — NX9500, NX9600

Syntax

```plaintext
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>** Configures a trustpoint name
  - **<TRUSTPOINT-NAME>** – Specify the trustpoint’s name.

- **secret [0 <WORD>|2 <WORD>]** Configures the secret used to encrypt the trustpoint. The secret should not exceed 128 characters in length.
  - **0 <WORD>** – Configures a clear text password
  - **2 <WORD>** – Configures an encrypted password

- **reference-id <WORD>** Configures the reference ID. The CA server uses this information to identify the shared secret key used.
  - **<WORD>** – Specify the reference ID.

- **sender-name <WORD>** 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.
  - **<WORD>** – Specify the sender name.

- **recipient-name** 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.
- **ca-psk <CERT-PATH>** Configures the certificate path for the server certificate
  - **<CERT-PATH>** – Specify the certificate path.
Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#trustpoint cmp-test subject-name "CN=ALCATEL-LUCENT.com,0=Alcatel Lucent" secret 0 test-secret reference-id 123456 sender-name "CN=ALCATEL-LUCENT.com,0=Alcatel Lucent" recipient-name "O=Alcatel Lucent,CN=ALU.com"
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
  ca-server host 192.168.8.74 port 80 path cmp
trustpoint cmp-test subject-name "CN=ALCATEL-LUCENT.com,0=Alcatel Lucent" secret 0 test-secret reference-id 123456 sender-name "CN=ALCATEL-LUCENT.com,0=Alcatel Lucent" recipient-name "O=Alcatel Lucent,CN=ALU.com"
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the trustpoint associated with this crypto CMP policy</td>
</tr>
</tbody>
</table>
29.1.3 use

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 5.5 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 — AP6522, WiMod
- Service Platforms — NX9500, NX9600

**Syntax**

```
use autogen-uniqueid
```

**Parameters**

- `use autogen-uniqueid`

**Examples**

```
ap6522-D8273A(config-cmp-policy-CMP)#use autogen-uniqueid

ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
use autogen-uniqueid
csa-server host 192.168.8.74 port 80 path cmp
trustpoint cmp-test subject-name "CN=ALCATEL-LUCENT.com,O=Alcatel Lucent" secret 0 test-secret reference-id 123456 sender-name "CN=ALCATEL-LUCENT.com,O=Alcatel Lucent" recipient-name "O=Alcatel Lucent,CN=ALU.com"
ap6522-D8273A(config-cmp-policy-CMP)#
```

**Related Commands**

- `no` Removes the device’s autogen-uniqueid associated with this crypto CMP policy
29.1.4 no

- crypto-cmp-policy-instance

Removes or reverts this crypto CMP policy settings

Supported in the following platforms:
- Access Points — AP6522, WiMod
- Service Platforms — NX9500, NX9600

Syntax
no [ca-server|trustpoint|use]

Parameters
- no [ca-server|trustpoint|use]

| no ca-server | Removes the configured CA server |
| no trustpoint | Removes the trustpoint associated with this crypto CMP policy |
| no use | Removes the device’s autogen-uniqueid associated with this crypto CMP policy |

Examples
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy_CMP
use autogen-uniqueid
crypto-cmp-policy_CMP
ca-server host 192.168.8.74 port 80 path cmp
trustpoint cmp-test subject-name "CN=ALCATEL-LUCENT.com,O=Alcatel Lucent" secret 0 test-secret reference-id 123456 sender-name "CN=ALCATEL-LUCENT.com,O=Alcatel Lucent" recipient-name "O=Alcatel Lucent,CN=ALU.com"
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#no ca-server

Related Commands
- ca-server Configures the CA server details
- trustpoint 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
- use Associates a device’s autogen-uniqueid with this crypto CMP policy
29.2 other-cmp-related-commands

Table 29.2 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 29-9</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 29-10</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 — AP6522, WiMod
- Service Platforms — NX9500, NX9600

Syntax
```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

Parameters
- `use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmp-policy &lt;CRYPTO-CMP-POLICY-NAME&gt;</td>
<td>Applies an existing CMP policy on this device</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;CRYPTO-CMP-POLICY-NAME&gt;</code> – 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 write
```
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 — AP6522, WiMod
- Service Platforms — NX9500, NX9600

Syntax

show crypto [cmp|pki]

show crypto cmp requests status
show crypto pki trustpoints

Parameters

- show crypto cmp requests status
  - show crypto cmp requests
    - Displays the current status of all on-going CMP requests
  - show crypto pki trustpoints
    - Displays all trustpoints including CMP generated trustpoints

Examples

ap6522-D8273A#show crypto pki trustpoints

<table>
<thead>
<tr>
<th>TRUSTPOINT</th>
<th>KEY NAME</th>
<th>VALID UNTIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmp-test</td>
<td>cmp-test-key</td>
<td>Fri May 9 09:44:22 2014 GMT</td>
</tr>
<tr>
<td>default-trustpoint</td>
<td>default_rsa_key</td>
<td>Fri Dec 30 00:00:40 2022 GMT</td>
</tr>
</tbody>
</table>

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:

```
<DEVICE>(config)#roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>
rfs6000-81742D(config)#roaming-assist-policy test
rfs6000-81742D(config-roaming-assist-policy-test)#?
```

**Roaming Assist Mode commands:**

- **action** Configure action - action is either to log / deauth
- **aggressiveness** Configure the roaming aggressiveness for a wireless client
- **detection-threshold** Configure the detection threshold - when exceeded, client monitoring starts
- **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 rss1 values are checked

```
clrscr
commit
end
exit
help
revert
service
show
write
```

```
rfs6000-81742D(config-roaming-assist-policy-test)#
```
30.1 roaming-assist-policy-instance

Table 30.1 summarizes roaming assist policy configuration 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 30-3</td>
</tr>
<tr>
<td>aggressiveness</td>
<td>Configures a roaming aggressiveness value for wireless clients</td>
<td>page 30-4</td>
</tr>
<tr>
<td>detection-threshold</td>
<td>Configures the detection-threshold value</td>
<td>page 30-5</td>
</tr>
<tr>
<td>handoff-count</td>
<td>Configures the handoff-count value</td>
<td>page 30-6</td>
</tr>
<tr>
<td>handoff-threshold</td>
<td>Configures the handoff-threshold value</td>
<td>page 30-7</td>
</tr>
<tr>
<td>monitoring interval</td>
<td>Configures the monitoring interval on the clients</td>
<td>page 30-8</td>
</tr>
<tr>
<td>sampling interval</td>
<td>Configures the sampling interval on the clients</td>
<td>page 30-9</td>
</tr>
<tr>
<td>no</td>
<td>Removes or reverts this roaming assist policy settings based on the parameters passed</td>
<td>page 30-10</td>
</tr>
</tbody>
</table>
30.1.1 action

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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

action [deauth|log]

Parameters

- action [deauth|log]

| action | deauth|log | Configures the action to be invoked on the client once it reaches the specified threshold value. In both cases an event is generated, the messages are different based on the action. |
|--------|-------|----------------------------------|
|        | deauth | The client is deauthenticated |
|        | log    | The log is generated |

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 a relatively low RSSI, resulting in a decaying-average 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, AP81XX, AP82XX
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX4500, NX4524, 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]

Examples

```bash
nx9500-6C8809(config-roaming-assist-policy-test)#aggressiveness medium
```

```bash
nx9500-6C8809(config-roaming-assist-policy-test)#show context roaming-assist-policy test
tagressiveness medium
```

```bash
nx9500-6C8809(config-roaming-assist-policy-test)#
```

Related Commands

```bash
no
```

Reverts the aggressiveness value to default (lowest)
30.1.3 **detection-threshold**

- **roaming-assist-policy-instance**

Specifies the detection-threshold determining when a client is monitored.

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

detection-threshold <-100--40>

**Parameters**

- detection-threshold <-100--40>

<table>
<thead>
<tr>
<th>detection-threshold &lt;-100--40&gt;</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></td>
<td>• &lt;-100--40&gt; – Specify the received signal strength indicator (rssi) value between -100dBm and -40dBm</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 handoff-count

Specifies the number of trials a client is permitted before which an action is invoked.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax
handoff-count <1-10>

Parameters
- handoff-count <1-10>

<table>
<thead>
<tr>
<th>handoff-count &lt;1-10&gt;</th>
<th>Configures the number of trials a client is permitted before an action is invoked.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;1-10&gt; — Specify the integer value between 1 - 10 seconds</td>
</tr>
<tr>
<td></td>
<td>If the client 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-count 1
rfs6000-81742D(config-roaming-assist-policy-test)#

Related Commands

no
Removes the configured handoff-count details
### 30.1.5 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 — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

handoff-threshold <-100--40>

**Parameters**

- handoff-threshold <-100--40>

| handoff-threshold <-100--40> | Configures the handoff-threshold which specifies client status for handoff-action. Once exceeded an action is invoked.  
- <-100--40> — Specify the received signal strength indicator (rssi) value between -100dBm and -40dBm |

**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
### 30.1.6 monitoring interval

**roaming-assist-policy-instance**

Configures the monitoring interval to detect clients with a rssi below the handoff-threshold.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
monitoring interval <1-60>
```

**Parameters**

- **monitoring interval <1-60>**

<table>
<thead>
<tr>
<th>monitoring interval</th>
<th>Specifies how often clients are sampled to detect clients with a rssi above handoff-threshold.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-60&gt;</td>
<td>&lt;1-60&gt; — Specify the duration between 1- 60 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
### 30.1.7 sampling interval

*roaming-assist-policy-instance*

Configures the sampling interval for detecting the clients

Supported in the following platforms:

- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

**Syntax**

```
sampling interval <5-60>
```

**Parameters**

- `sampling interval <5-60>`

<table>
<thead>
<tr>
<th>sampling interval</th>
<th>Specifies how often clients are sampled to detect clients with a rssi above detection-threshold.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;5-60&gt;</td>
<td>• <code>&lt;5-60&gt;</code> – Specify the duration between 5 - 60 seconds. The default value is 15 seconds.</td>
</tr>
<tr>
<td></td>
<td>Note: The higher the RSSI number, the stronger the signal</td>
</tr>
</tbody>
</table>

**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
30.1.8 no

This command removes or reverts this roaming assist policy settings based on the parameters passed.

Supported in the following platforms:
- Access Points — AP300, 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, NX9000, NX9500, NX9510, NX9600

Syntax

no [action|aggressiveness|detection-threshold|handoff-count|handoff-threshold|handoff-threshold|monitoring-interval|sampling-interval]

Parameters
- no <PARAMETERS>

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)#
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

It is assumed you have a RFS4000 wireless controller with the latest build available. It is also assumed you have one AP650 model access point and one AP71XX model access point, both with the latest firmware available.

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 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.

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

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

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

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:

```bash
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.

```bash
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.

```bash
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#commit write
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#exit
```

To define the wireless controller’s physical location, use the same RF Domain configuration.

```bash
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
```

```bash
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.

```bash
rfs4000(config-device-03-14-28-57-14-28)#commit write
rfs4000(config-device-03-14-28-57-14-28)#exit
```

```bash
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:

```bash
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:

```bash
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.

```bash
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#exit
```

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.

```bash
rfs4000(config-profile-RFS4000_UseCase1)#interface ge 3
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#switchport access vlan 2
```

Map VLAN 2 to this interface. This assigns the IP address to the selected physical interface.

```bash
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#exit
```

Similarly, map the defined VLAN 2 to the GE4 interface.

```bash
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
```

```bash
rfs4000(config-profile-RFS4000_UseCase1)#
```
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.

```plaintext
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.

```plaintext
rfs4000(config-profile-AP650_UseCase1)#interface radio 1
rfs4000(config-profile-AP650_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-AP650_UseCase1-if-radio1)#exit
rfs4000(config-profile-AP650_UseCase1)#interface radio 2
rfs4000(config-profile-AP650_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-AP650_UseCase1-if-radio2)#exit
rfs4000(config-profile-AP650_UseCase1)#
```

Commit the changes made to this profile and exit.

```plaintext
rfs4000(config-profile-AP650_UseCase1)#commit write
rfs4000(config-profile-AP650_UseCase1)#exit
rfs4000(config)#
```

**Apply this Profile to the Discovered AP650**

Access the discovered access point using the following command. The discovered device’s MAC address is used to access its context.

```plaintext
rfs4000(config)#ap650 00-A0-F8-00-00-01
rfs4000(config-device-00-A0-F8-00-00-01)#
```

Assign the AP profile to this AP650 access point.

```plaintext
rfs4000(config-device-00-A0-F8-00-00-01)#use profile AP650_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#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 country code of its associated wireless controller.

```plaintext
rfs4000(config-device-00-A0-F8-00-00-01)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
rfs4000(config)#
```

### A.1.3.4.2 Creating an AP71XX Profile

**Creating an AP Profile**

To create a profile for use with an AP71XX:

```plaintext
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.

```plaintext
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.

```plaintext
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
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
```

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

**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)#
```
Table A.1 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
```

Configure the IP pool used with a network segment. This starts the DHCP server on the specified interface.

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#network 172.16.11.0/24
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#exit
```

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#exit
rfs4000-37FABE(config)#commit write
```

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
```

```
rfs4000-37FABE(config)#
```

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.
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
- AP8132
- AP8122
- AP7532
- AP7522
- AP7502
- AP7181
- AP7161
- AP7131
- AP6562
- AP6532
- AP6521
- AP6522
- AP6511
- AP650
- AP622
- AP621

**Wireless Switches**
- NX9510
- NX9500
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>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>
</tbody>
</table>

For more information visit [www.zebra.com/support](http://www.zebra.com/support).
<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>URL</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge</td>
<td>1.0.4</td>
<td><a href="http://www.linuxfoundation.org/collaborate/">http://www.linuxfoundation.org/collaborate/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>workgroups/networking/bridge/</td>
<td></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>dash</td>
<td>0.5.7</td>
<td><a href="http://gondor.apana.org.au/~herbert/dash/">http://gondor.apana.org.au/~herbert/dash/</a></td>
<td>The BSD License</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.thekellesys.org.uk/dnsmasq/doc.html">http://www.thekellesys.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>gcc</td>
<td>4.1.2</td>
<td><a href="http://gcc.gnu.org/">http://gcc.gnu.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>gdb</td>
<td>7.2</td>
<td><a href="http://www.gnu.org/software/gdb/">http://www.gnu.org/software/gdb/</a></td>
<td>GNU General Public License, version 3</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>gdbm</td>
<td>1.8.3</td>
<td><a href="http://www.gnu.org/s/gdbm/">http://www.gnu.org/s/gdbm/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>genext2fs</td>
<td>1.4.1</td>
<td><a href="http://genext2fs.sourceforge.net/">http://genext2fs.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</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>glibc</td>
<td>2.7</td>
<td><a href="http://www.gnu.org/software/libc/">http://www.gnu.org/software/libc/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>hdparm</td>
<td>9.38</td>
<td><a href="http://sourceforge.net/projects/hdparm/">http://sourceforge.net/projects/hdparm/</a></td>
<td>GNU General Public License, version 2</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>hotplug2</td>
<td>0.9</td>
<td><a href="http://isteve.bofh.cz/~isteve/hotplug2/">http://isteve.bofh.cz/~isteve/hotplug2/</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>ipaddr</td>
<td>2.1.0</td>
<td><a href="http://code.google.com/p/ipaddr-py/">http://code.google.com/p/ipaddr-py/</a></td>
<td>Apache License, Version 2.0</td>
</tr>
<tr>
<td>ipkg-utils</td>
<td>1.7</td>
<td><a href="http://www.handhelds.org/sources.html">http://www.handhelds.org/sources.html</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>ipmitool</td>
<td>1.8.11</td>
<td><a href="http://ipmitool.sourceforge.net/">http://ipmitool.sourceforge.net/</a></td>
<td>The BSD License</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>kexec-tools</td>
<td>2.0.3</td>
<td><a href="http://kernel.org/pub/linux/utils/kernel/kexec/">http://kernel.org/pub/linux/utils/kernel/kexec/</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>ftp://sources.redhat.com/pub/lvm2/old</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>libexpat</td>
<td>2.0.0</td>
<td><a href="http://expat.sourceforge.net/">http://expat.sourceforge.net/</a></td>
<td>MIT License</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>libnettle</td>
<td>2.4</td>
<td><a href="http://www.lysator.liu.se/~nisse/nettle/">http://www.lysator.liu.se/~nisse/nettle/</a></td>
<td>GNU Lesser General Public License 2.1</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/rltop.html">http://cnswww.cns.cwru.edu/php/chet/readline/rltop.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>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>----------------------------------------------</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>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="http://ltp.sourceforge.net/">http://ltp.sourceforge.net/</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>lzo</td>
<td>2.03</td>
<td><a href="http://www.oberhumer.com/opensource/lzo/">http://www.oberhumer.com/opensource/lzo/</a></td>
<td>GNU General Public License, version 2</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>mii-diag</td>
<td>2.09</td>
<td><a href="http://freecode.com/projects/mii-diag">http://freecode.com/projects/mii-diag</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>mkyaafs</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>mtd</td>
<td>2009-05-05</td>
<td><a href="http://www.linux-mtd.infradead.org/">http://www.linux-mtd.infradead.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Version</strong></td>
<td><strong>URL</strong></td>
<td><strong>License</strong></td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------</td>
<td>-------------</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>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>Open SSL License</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>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>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------</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>portmap</td>
<td>6.0</td>
<td><a href="http://neil.brown.name/portmap/">http://neil.brown.name/portmap/</a></td>
<td>The BSD License</td>
</tr>
<tr>
<td>ppp</td>
<td>2.4.5</td>
<td><a href="http://ppp.samba.org/">http://ppp.samba.org/</a></td>
<td>The BSD License</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>proclname</td>
<td>0.2</td>
<td><a href="http://code.google.com/p/proclname/">http://code.google.com/p/proclname/</a></td>
<td>GNU Lesser General Public License, version 2</td>
</tr>
<tr>
<td>proclps</td>
<td>3.2.8</td>
<td><a href="http://proclps.sourceforge.net/">http://proclps.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</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>pyparseing</td>
<td>1.5.1</td>
<td><a href="http://sourceforge.net/projects/pyparseing">http://sourceforge.net/projects/pyparseing</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>qdbm</td>
<td>1.8.77</td>
<td><a href="http://qdbm.sourceforge.net/">http://qdbm.sourceforge.net/</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/pppoe">http://www.roaringpenguin.com/products/pppoe</a></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>safestr</td>
<td>1.0.3</td>
<td><a href="http://www.zork.org/">http://www.zork.org/</a></td>
<td>The BSD License</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>sed</td>
<td>4.1.2</td>
<td><a href="http://www.gnu.org/software/sed/">http://www.gnu.org/software/sed/</a></td>
<td>GNU General Public License, version 2</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>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------</td>
<td>----------------------------------------</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>3070900</td>
<td><a href="http://www.sqlite.org/">http://www.sqlite.org/</a></td>
<td>None</td>
</tr>
<tr>
<td>squashfs</td>
<td>3.0</td>
<td><a href="http://squashfs.sourceforge.net/">http://squashfs.sourceforge.net/</a></td>
<td>GNU General Public License, version 2</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>stunnel</td>
<td>4.31</td>
<td><a href="http://www.stunnel.org/">http://www.stunnel.org/</a></td>
<td>GNU General Public License, version 2</td>
</tr>
<tr>
<td>sysstat</td>
<td>9.0.5</td>
<td><a href="http://sebastien.godard.pagesperso-orange.fr/">http://sebastien.godard.pagesperso-orange.fr/</a></td>
<td>GNU General Public License, version 2</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>Name</td>
<td>Version</td>
<td>URL</td>
<td>License</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------------------------------------------</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_Touriilhes/Linux/Tools.html">http://www.hpl.hp.com/personal/Jean_Touriilhes/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>wuftpdl</td>
<td>1.0.21</td>
<td><a href="http://wu-ftpd.therockgarden.ca/">http://wu-ftpd.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-analyserr</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>xen-tools</td>
<td>4.2.1</td>
<td><a href="http://xen-tools.org/software/xen-tools/">http://xen-tools.org/software/xen-tools/</a></td>
<td>GNU General Public License, version 2</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, ALL OF WHICH 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 work 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 strlcat() (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.

strlcat() 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 the GNU 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 i 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, selling, or otherwise propagating the contents of 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 convey 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.
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 runtime 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
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.

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.

END OF TERMS AND CONDITIONS
B.3.11 GNU Lesser General Public License, version 2.0

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.

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 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.

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 "wuftpd" 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
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:

- **MAC ID 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 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**

To see manuals, go to: www.zebra.com/support.