EX-3524/EX-3548
Layer 2 Gigabit Ethernet PoE/PoE+ Switch
CLI Reference Guide
This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read this Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How this Guide is Organized

This guide describes the switch's command line interface (CLI). For more detailed information on the switch's key features refer to the System Reference Guide.

The guide includes these sections:

- Section I "Getting Started" — Includes information on initial configuration.
- Section II "Command Line Interface" — Includes all management options available through the CLI.
- Section III "Appendices" — Includes information on troubleshooting switch management access.

Related Documentation

This guide focuses on switch software configuration through the CLI.

For information on how to manage the switch through the Web management interface, see the following guide:

System Reference Guide

For information on how to install the switch, see the following guide:

Installation Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide
Safety and Regulatory Information
How to Use This Guide

Conventions  The following conventions are used throughout this guide to show information:

- **Note:** Emphasizes important information or calls your attention to related features or instructions.

- **Caution:** Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

- **Warning:** Alerts you to a potential hazard that could cause personal injury.

Revision History  This section summarizes the changes in each revision of this guide.

**December 2014 Revision**
This is the third version of this guide. This guide is valid for software release v5.0.0.0-07D. This release includes a major change in the underlying software platform. It contains the following changes:

- Updated data displayed by the commands "show access-list tcam-utilization" on page 99, "show memory" on page 100, and "show process cpu" on page 100.

- Updated syntax for "show running-config" on page 101.

- Added the command "show tech-support" on page 104.

- Updated display output for the command "show version" on page 106.

- Added the commands "show watchdog" on page 107 and "watchdog software" on page 107.

- Updated syntax for the command "copy" on page 110.

- Updated syntax for the command "delete" on page 113.

- Added the command "upgrade opcode reload" on page 118.

- Added the section "TFTP Configuration Commands" on page 118.

- Removed the "auto" option from the command "speed" on page 127.

- Added the command "terminal" on page 129.

- Updated display output for the command "show line" on page 130.
◆ Updated syntax for the commands "logging host" on page 133 and "logging sendmail host" on page 138.

◆ Added the section "NTP Commands" on page 145.

◆ Added the commands "clock summer-time (predefined)" on page 150 and "clock summer-time (recurring)" on page 151.

◆ Removed the command “clock timezone-predefined” from the section "Manual Configuration Commands" on page 149.

◆ Added the section "Adopt Device" on page 164.

◆ Updated syntax for the command "snmp-server enable traps" on page 176.

◆ Added the commands "snmp-server enable port-traps mac-notification" on page 179 and "show snmp-server enable port-traps" on page 180.

◆ Added the section "Additional Trap Commands" on page 192.

◆ Updated description of “level” parameter for the command "enable password" on page 204.

◆ Updated description of “access level” parameter for the command "username" on page 205.

◆ Added the commands "privilege" on page 207 and "show privilege" on page 207.

◆ Updated syntax for the command "tacacs-server host" on page 215.

◆ Added the commands "tacacs-server retransmit" on page 216 and "tacacs-server timeout" on page 217.

◆ Added the commands "aaa accounting commands" on page 219 and "accounting commands" on page 225.

◆ Updated syntax for the command "show accounting" on page 228.

◆ Added the command "dot1x max-reauth-req" on page 248.

◆ Added the section "PPPoE Intermediate Agent" on page 262.

◆ Added the command "mac-learning" on page 272.

◆ Added the command "show port security" on page 275.

◆ Updated syntax for the command "ip dhcp snooping information option" on page 299.
How to Use This Guide

- Added the commands "ip dhcp snooping information option encode no-subtype" on page 300, "ip dhcp snooping information option remote-id" on page 301, "ip dhcp snooping limit rate" on page 303, and "ip dhcp snooping information option circuit-id" on page 305.

- Updated display output for the command "show ip dhcp snooping" on page 308.

- Added the section "DHCPv6 Snooping" on page 309.

- Updated syntax for the commands "ip source-guard binding" on page 319 and "ip source-guard max-binding" on page 323.

- Added the command "clear ip source-guard binding blocked" on page 323.

- Added the command "ip source-guard mode" on page 324.

- Updated syntax for the command "show ip source-guard binding" on page 325.

- Added the section "IPv6 Source Guard" on page 326.

- Added “allow-zeros” parameter to the command "ip arp inspection validate" on page 335.

- Updated command in the section "Denial of Service Protection" on page 340.

- Updated command in the section "Port-based Traffic Segmentation" on page 346.

- Removed “redirect-to” interface options from all permit and deny commands in the chapter "Access Control Lists" on page 351.

- Removed “tos” parameter from the command "permit, deny (Extended IPv4 ACL)" on page 354.

- Added “counter” parameter to the commands "ip access-group" on page 356, "ipv6 access-group" on page 362 and "mac access-group" on page 369.

- Updated syntax for the command "permit, deny(MAC ACL)" on page 365.

- Added “log” parameter to the command "permit, deny (ARP ACL)" on page 371.

- Added the command "clear access-list hardware counters" on page 373, and added “hardware counters” parameter to the command "show access-list" on page 374.

- Removed the “symmetric” parameter from the command "capabilities" on page 379.
◆ Added the command "media-type" on page 382.
◆ Removed the command "giga-phy-mode" from the chapter "Interface Commands" on page 377.
◆ Updated display output for the command "show interfaces status" on page 388.
◆ Added the section "Transceiver Threshold Configuration" on page 390.
◆ Added the command "port-channel load-balance" on page 404, "lACP timeout" on page 411, and "show port-channel load-balance" on page 415.
◆ Added the commands "power mainpower maximum allocation" on page 418 and "show power mainpower" on page 424.
◆ Removed the command "show power poe" from the chapter "Power over Ethernet Commands" on page 417.
◆ Updated syntax for the command "port monitor" on page 425.
◆ Reduced the maximum number of mirror sessions from two to one for all relevant local mirror and remote mirror commands in the chapter "Port Mirroring Commands" on page 425.
◆ Added the chapter "Loopback Detection Commands" on page 453.
◆ Added the command "spanning-tree system-bpdu-flooding" on page 472.
◆ Updated syntax for the command "spanning-tree bpdu-guard" on page 478.
◆ Updated syntax for the command "spanning-tree loopback-detection action" on page 482.
◆ Added the command "spanning-tree port-bpdu-flooding" on page 486.
◆ Added the command "spanning-tree tc-prop-stop" on page 488.
◆ Updated syntax for the command "show spanning-tree" on page 490.
◆ Added the command "switchport dot1q-tunnel service match cvid" on page 518.
◆ Updated syntax and display output for the command "show dot1q-tunnel" on page 520.
◆ Added the section "Configuring L2CP Tunneling" on page 521.
◆ Added the “priority” parameter to the command "protocol-vlan protocol-group (Configuring Interfaces)" on page 527.
How to Use This Guide

- Added the “mask” parameter to the command "mac-vlan" on page 532.
- Added the “match-all” option to the command "class-map" on page 554.
- Updated syntax for the command "match" on page 556.
- Updated range for "Quality of Service Commands" on page 553.
- Added the command "ip igmp snooping priority" on page 574.
- Added the commands "clear ip igmp snooping groups dynamic" on page 588 and "clear ip igmp snooping statistics" on page 589.
- Updated syntax for the command "show ip igmp snooping" on page 589 and "show ip igmp snooping group" on page 590.
- Added the sections "MLD Snooping" on page 608 and "MLD Filtering and Throttling" on page 621.
- Replaced command set for "Multicast VLAN Registration for IPv4" on page 630.
- Added the section "Multicast VLAN Registration for IPv6" on page 654.
- Added the command "lldp dot3-tlv mac-phy" on page 684.
- Removed the command “ipv6 dhcp client rapid-commit vlan” from the section "DHCP for IPv6" on page 716.
- Updated syntax for the command "ip address" on page 724.
- Added the command "traceroute6" on page 752.
- Added the command "ipv6 nd raguard" on page 757 and "show ipv6 nd raguard" on page 759.
- Added the section "ND Snooping" on page 761.
- Added the command "ip sw-route" on page 772.

September 2014 Revision
This is the second version of this guide. This guide is valid for software release v4.0.1.0-04R. It contains the following changes:

- Updated syntax description for the command "snmp-server user" on page 183.
How to Use This Guide

- Added the command "clear ip dhcp snooping binding" on page 307.
- Updated description for the command "spanning-tree bpdu-filter" on page 477.
- Updated usage information for the command "spanning-tree port-priority" on page 486.
- Updated syntax for the command "switchport trunk allowed vlan" on page 509.
- Updated syntax for the command "switchport trunk native vlan" on page 510.
- Added the commands "switchport trunk allowed vlan" on page 509 and "switchport trunk native vlan" on page 510.
- Updated configuration procedure for protocol-based VLANs. See "Configuring Protocol-based VLANs" on page 525.
- Updated command usage for "subnet-vlan" on page 530.
- Updated command usage for "mac-vlan" on page 532.
- Updated usage information for the command "voice vlan aging" on page 535.
- Updated usage information for the command "show voice vlan" on page 539.
- Added the command "show lldp neighbors" on page 696.
- Updated display text for the command “show cdp neighbors detail” on page 703.
- Changed default setting for the command "ip dhcp client class-id" on page 714.
- Removed the command “show ip dhcp client-identifier” on page 542.
- Updated output display for the command "show ip interface" on page 727.

March 2014 Revision
This is the first version of this guide. This guide is valid for software release v4.0.0.0-02R.
## Contents

<table>
<thead>
<tr>
<th>Section I</th>
<th>Getting Started</th>
<th>49</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Initial Switch Configuration</td>
<td></td>
<td>51</td>
</tr>
<tr>
<td>Connecting to the Switch</td>
<td></td>
<td>51</td>
</tr>
<tr>
<td>Configuration Options</td>
<td></td>
<td>51</td>
</tr>
<tr>
<td>Connecting to the Console Port</td>
<td></td>
<td>52</td>
</tr>
<tr>
<td>Logging Onto the Command Line Interface</td>
<td></td>
<td>53</td>
</tr>
<tr>
<td>Setting Passwords</td>
<td></td>
<td>53</td>
</tr>
<tr>
<td>Remote Connections</td>
<td></td>
<td>54</td>
</tr>
<tr>
<td>Configuring the Switch for Remote Management</td>
<td></td>
<td>55</td>
</tr>
<tr>
<td>Using the Network Interface</td>
<td></td>
<td>55</td>
</tr>
<tr>
<td>Setting an IP Address</td>
<td></td>
<td>55</td>
</tr>
<tr>
<td>Enabling SNMP Management Access</td>
<td></td>
<td>61</td>
</tr>
<tr>
<td>Managing System Files</td>
<td></td>
<td>63</td>
</tr>
<tr>
<td>Upgrading the Operation Code</td>
<td></td>
<td>64</td>
</tr>
<tr>
<td>Saving or Restoring Configuration Settings</td>
<td></td>
<td>65</td>
</tr>
<tr>
<td>Automatic Installation of Operation Code and Configuration Settings</td>
<td></td>
<td>66</td>
</tr>
<tr>
<td>Downloading Operation Code from a File Server</td>
<td></td>
<td>66</td>
</tr>
<tr>
<td>Specifying a DHCP Client Identifier</td>
<td></td>
<td>69</td>
</tr>
<tr>
<td>Downloading a Configuration File Referenced by a DHCP Server</td>
<td></td>
<td>69</td>
</tr>
<tr>
<td>Setting the System Clock</td>
<td></td>
<td>71</td>
</tr>
<tr>
<td>Setting the Time Manually</td>
<td></td>
<td>72</td>
</tr>
<tr>
<td>Configuring SNTP</td>
<td></td>
<td>72</td>
</tr>
</tbody>
</table>
Section II  Command Line Interface  75

2  Using the Command Line Interface  77

Accessing the CLI  77
  Console Connection  77
  Telnet Connection  78

Entering Commands  79
  Keywords and Arguments  79
  Minimum Abbreviation  79
  Command Completion  79

Getting Help on Commands  80
  Partial Keyword Lookup  82

Negating the Effect of Commands  82

Using Command History  82

Understanding Command Modes  82

Exec Commands  83

Configuration Commands  83

Command Line Processing  85

CLI Command Groups  86

3  General Commands  89

  prompt  89
  reload (Global Configuration)  90
  enable  91
  quit  92
  show history  92
  configure  93
  disable  94
  reload (Privileged Exec)  94
  show reload  95
  end  95
  exit  95
4 System Management Commands

Device Designation

hostname

System Status

show access-list tcam-utilization
show memory
show process cpu
show running-config
show startup-config
show system
show tech-support
show users
show version
show watchdog
watchdog software

Frame Size

jumbo frame

File Management

General Commands

boot system

Automatic Code Upgrade Commands

upgrade opcode auto
upgrade opcode path
upgrade opcode reload
show upgrade

TFTP Configuration Commands

ip tftp retry
ip tftp timeout
show ip tftp

Line

line
NTP Commands 145
  ntp authenticate 145
  ntp authentication-key 146
  ntp client 147
  ntp server 147
  show ntp 148

Manual Configuration Commands 149
  clock summer-time (date) 149
  clock summer-time (predefined) 150
  clock summer-time (recurring) 151
  clock timezone 153
  calendar set 153
  show calendar 154

Time Range 155
  time-range 155
  absolute 156
  periodic 157
  show time-range 158

Switch Clustering 158
  cluster 159
  cluster commander 160
  cluster ip-pool 161
  cluster member 161
  rcommand 162
  show cluster 163
  show cluster members 163
  show cluster candidates 163

Adopt Device 164
  controller hello-interval adjacency-hold-time 166
  controller host ip address 166
  adoptd upgrade 167
  debug adoption 168
  no adoption 168
  show adoption debug 168
  show adoption history 169
show adoption status 170

5 SNMP Commands 171

General SNMP Commands 173

snmp-server 173
snmp-server community 173
snmp-server contact 174
snmp-server location 175
show snmp 175

SNMP Target Host Commands 176

snmp-server enable traps 176
snmp-server host 177
snmp-server enable port-traps mac-notification 179
show snmp-server enable port-traps 180

SNMPv3 Commands 181

snmp-server engine-id 181
snmp-server group 182
snmp-server user 183
snmp-server view 185
show snmp engine-id 186
show snmp group 186
show snmp user 187
show snmp view 188

Notification Log Commands 189

nlm 189
snmp-server notify-filter 190
show nlm oper-status 191
show snmp notify-filter 191

Additional Trap Commands 192

memory 192
process cpu 192

6 Remote Monitoring Commands 195

rmon alarm 196
rmon event 197
rmon collection history 198
aaa authorization commands 222
aaa authorization exec 223
aaa group server 224
server 224
accounting dot1x 225
accounting commands 225
accounting exec 226
authorization commands 227
authorization exec 227
show accounting 228

Web Server 229
ip http port 229
ip http server 230
ip http secure-port 230
ip http secure-server 231

Telnet Server 232
ip telnet max-sessions 233
ip telnet port 233
ip telnet server 234
show ip telnet 234

Secure Shell 234
ip ssh authentication-retries 237
ip ssh server 238
ip ssh server-key size 239
ip ssh timeout 239
delete public-key 240
ip ssh crypto host-key generate 240
ip ssh crypto zeroize 241
ip ssh save host-key 242
show ip ssh 242
show public-key 243
show ssh 244

802.1X Port Authentication 244
General Commands 245
dot1x default 245
dot1x eapol-pass-through 246
dot1x system-auth-control 247

Authenticator Commands 247
dot1x intrusion-action 247
dot1x max-reauth-req 248
dot1x max-req 248
dot1x operation-mode 249
dot1x port-control 250
dot1x re-authentication 250
dot1x timeout quiet-period 251
dot1x timeout re-authperiod 251
dot1x timeout supp-timeout 252
dot1x timeout tx-period 252
dot1x re-authenticate 253

Supplicant Commands 254
dot1x identity profile 254
dot1x max-start 254
dot1x pae supplicant 255
dot1x timeout auth-period 256
dot1x timeout held-period 256
dot1x timeout start-period 257

Information Display Commands 257
show dot1x 257

Management IP Filter 260
management 260
show management 261

PPPoE Intermediate Agent 262
pppoe intermediate-agent 263
pppoe intermediate-agent format-type 263
pppoe intermediate-agent port-enable 264
pppoe intermediate-agent port-format-type 265
pppoe intermediate-agent port-format-type remote-id-delimiter 266
pppoe intermediate-agent trust 266
pppoe intermediate-agent vendor-tag strip 267
clear pppoe intermediate-agent statistics 267
8 General Security Measures 271
Port Security 272
mac-learning 272
port security 273
show port security 275
Network Access (MAC Address Authentication) 277
network-access aging 278
network-access mac-filter 278
mac-authentication reauth-time 279
network-access dynamic-qos 280
network-access dynamic-vlan 281
network-access guest-vlan 282
network-access link-detection 282
network-access link-detection link-down 283
network-access link-detection link-up 283
network-access link-detection link-up-down 284
network-access max-mac-count 284
network-access mode mac-authentication 285
network-access port-mac-filter 286
mac-authentication intrusion-action 287
mac-authentication max-mac-count 287
clear network-access 288
show network-access 288
show network-access mac-address-table 289
show network-access mac-filter 290
Web Authentication 290
web-auth login-attempts 291
web-auth quiet-period 292
web-auth session-timeout 292
web-auth system-auth-control 293
web-auth 293
web-auth re-authenticate (Port) 294
web-auth re-authenticate (IP) 294
show web-auth 295
show web-auth interface 295
show web-auth summary 296

DHCPv4 Snooping 296
ip dhcp snooping 297
ip dhcp snooping information option 299
ip dhcp snooping information option encode no-subtype 300
ip dhcp snooping information option remote-id 301
ip dhcp snooping information policy 302
ip dhcp snooping limit rate 303
ip dhcp snooping verify mac-address 303
ip dhcp snooping vlan 304
ip dhcp snooping information option circuit-id 305
ip dhcp snooping trust 306
clear ip dhcp snooping binding 307
clear ip dhcp snooping database flash 307
ip dhcp snooping database flash 308
show ip dhcp snooping 308
show ip dhcp snooping binding 309

DHCPv6 Snooping 309
ipv6 dhcp snooping 310
ipv6 dhcp snooping option remote-id 312
ipv6 dhcp snooping option remote-id policy 313
ipv6 dhcp snooping vlan 314
ipv6 dhcp snooping max-binding 315
ipv6 dhcp snooping trust 315
clear ipv6 dhcp snooping binding 316
clear ipv6 dhcp snooping statistics 317
show ipv6 dhcp snooping 317
show ipv6 dhcp snooping binding 318
show ipv6 dhcp snooping statistics 318

IPv4 Source Guard 319
ip source-guard binding 319
ip source-guard 321
ip source-guard max-binding 323
clear ip source-guard binding blocked 323
ip source-guard mode 324
show ip source-guard 325
show ip source-guard binding 325
IPv6 Source Guard 326
ipv6 source-guard binding 326
ipv6 source-guard 328
ipv6 source-guard max-binding 329
show ipv6 source-guard 330
show ipv6 source-guard binding 331
ARP Inspection 331
ip arp inspection 332
ip arp inspection filter 333
ip arp inspection log-buffer logs 334
ip arp inspection validate 335
ip arp inspection vlan 336
ip arp inspection limit 337
ip arp inspection trust 337
show ip arp inspection configuration 338
show ip arp inspection interface 338
show ip arp inspection log 339
show ip arp inspection statistics 339
show ip arp inspection vlan 340
Denial of Service Protection 340
dos-protection echo-chargen 341
dos-protection smurf 341
dos-protection tcp-flooding 342
dos-protection tcp-null-scan 342
dos-protection tcp-syn-fin-scan 343
dos-protection tcp-udp-port-zero 343
dos-protection tcp-xmas-scan 344
dos-protection udp-flooding 344
dos-protection win-nuke 345
show dos-protection 345
Port-based Traffic Segmentation

<table>
<thead>
<tr>
<th>Traffic Segmentation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-segmentation</td>
<td>346</td>
</tr>
<tr>
<td>traffic-segmentation session</td>
<td>347</td>
</tr>
<tr>
<td>traffic-segmentation uplink/downlink</td>
<td>348</td>
</tr>
<tr>
<td>traffic-segmentation uplink-to-uplink</td>
<td>349</td>
</tr>
<tr>
<td>show traffic-segmentation</td>
<td>350</td>
</tr>
</tbody>
</table>

9 Access Control Lists

<table>
<thead>
<tr>
<th>Access Control Lists</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 ACLs</td>
<td>351</td>
</tr>
<tr>
<td>access-list ip</td>
<td>352</td>
</tr>
<tr>
<td>permit, deny (Standard IP ACL)</td>
<td>353</td>
</tr>
<tr>
<td>permit, deny (Extended IPv4 ACL)</td>
<td>354</td>
</tr>
<tr>
<td>ip access-group</td>
<td>356</td>
</tr>
<tr>
<td>show ip access-group</td>
<td>357</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>357</td>
</tr>
<tr>
<td>IPv6 ACLs</td>
<td>358</td>
</tr>
<tr>
<td>access-list ipv6</td>
<td>358</td>
</tr>
<tr>
<td>permit, deny (Standard IPv6 ACL)</td>
<td>359</td>
</tr>
<tr>
<td>permit, deny (Extended IPv6 ACL)</td>
<td>360</td>
</tr>
<tr>
<td>ipv6 access-group</td>
<td>362</td>
</tr>
<tr>
<td>show ipv6 access-group</td>
<td>363</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>363</td>
</tr>
<tr>
<td>MAC ACLs</td>
<td>364</td>
</tr>
<tr>
<td>access-list mac</td>
<td>364</td>
</tr>
<tr>
<td>permit, deny (MAC ACL)</td>
<td>365</td>
</tr>
<tr>
<td>mac access-group</td>
<td>369</td>
</tr>
<tr>
<td>show mac access-group</td>
<td>369</td>
</tr>
<tr>
<td>show mac access-list</td>
<td>370</td>
</tr>
<tr>
<td>ARP ACLs</td>
<td>370</td>
</tr>
<tr>
<td>access-list arp</td>
<td>370</td>
</tr>
<tr>
<td>permit, deny (ARP ACL)</td>
<td>371</td>
</tr>
<tr>
<td>show access-list arp</td>
<td>372</td>
</tr>
<tr>
<td>show arp access-list</td>
<td>373</td>
</tr>
<tr>
<td>ACL Information</td>
<td>373</td>
</tr>
<tr>
<td>clear access-list hardware counters</td>
<td>373</td>
</tr>
</tbody>
</table>
show access-group 374
show access-list 374

10 Interface Commands 377

Interface Configuration 378
interface 378
alias 379
capabilities 379
description 381
flowcontrol 381
media-type 382
negotiation 383
shutdown 383
speed-duplex 384
clear counters 385
show interfaces brief 386
show interfaces counters 386
show interfaces status 388
show interfaces switchport 389

Transceiver Threshold Configuration 390
transceiver-monitor 390
transceiver-threshold-auto 391
transceiver-threshold current 391
transceiver-threshold rx-power 393
transceiver-threshold temperature 394
transceiver-threshold tx-power 395
transceiver-threshold voltage 396
show interfaces transceiver 397
show interfaces transceiver-threshold 398

Cable Diagnostics 399
test cable-diagnostics 399
show cable-diagnostics 400

Power Savings 401
power-save 401
show power-save 402
### 11 Link Aggregation Commands

#### Manual Configuration Commands
- `port-channel load-balance`
- `channel-group`

#### Dynamic Configuration Commands
- `lacp`
- `lacp admin-key (Ethernet Interface)`
- `lacp port-priority`
- `lacp system-priority`
- `lacp admin-key (Port Channel)`
- `lacp timeout`

#### Trunk Status Display Commands
- `show lacp`
- `show port-channel load-balance`

### 12 Power over Ethernet Commands

- `power inline compatible`
- `power mainpower maximum allocation`
- `power inline`
- `power inline maximum allocation`
- `power inline priority`
- `power inline time-range`
- `show power inline status`
- `show power inline time-range`
- `show power mainpower`

### 13 Port Mirroring Commands

#### Local Port Mirroring Commands
- `port monitor`
- `show port monitor`

#### RSPAN Mirroring Commands
- `rspan source`
- `rspan destination`
- `rspan remote vlan`
- `no rspan session`
- `show rspan`
14 Congestion Control Commands

Rate Limit Commands

rate-limit

Storm Control Commands

switchport packet-rate

Automatic Traffic Control Commands

Threshold Commands

auto-traffic-control apply-timer
auto-traffic-control release-timer
auto-traffic-control
auto-traffic-control action
auto-traffic-control alarm-clear-threshold
auto-traffic-control alarm-fire-threshold
auto-traffic-control auto-control-release
auto-traffic-control control-release

SNMP Trap Commands

snmp-server enable port-traps atc broadcast-alarm-clear
snmp-server enable port-traps atc broadcast-alarm-fire
snmp-server enable port-traps atc broadcast-control-apply
snmp-server enable port-traps atc broadcast-control-release
snmp-server enable port-traps atc multicast-alarm-clear
snmp-server enable port-traps atc multicast-alarm-fire
snmp-server enable port-traps atc multicast-control-apply
snmp-server enable port-traps atc multicast-control-release

ATC Display Commands

show auto-traffic-control
show auto-traffic-control interface

15 Loopback Detection Commands

loopback-detection
loopback-detection action
loopback-detection recover-time
loopback-detection transmit-interval
loopback detection trap
loopback-detection release
16 Address Table Commands

- show loopback-detection
- mac-address-table aging-time
- mac-address-table static
- clear mac-address-table dynamic
- show mac-address-table
- show mac-address-table aging-time
- show mac-address-table count

17 Spanning Tree Commands

- spanning-tree
- spanning-tree cisco-prestandard
- spanning-tree forward-time
- spanning-tree hello-time
- spanning-tree max-age
- spanning-tree mode
- spanning-tree pathcost method
- spanning-tree priority
- spanning-tree mst configuration
- spanning-tree system-bpdu-flooding
- spanning-tree transmission-limit
- max-hops
- mst priority
- mst vlan
- name
- revision
- spanning-tree bpdu-filter
- spanning-tree bpdu-guard
- spanning-tree cost
- spanning-tree edge-port
- spanning-tree link-type
- spanning-tree loopback-detection
- spanning-tree loopback-detection action
- spanning-tree loopback-detection release-mode
- spanning-tree loopback-detection trap
18 VLAN Commands 495

GVRP and Bridge Extension Commands 496
  bridge-ext gvrp 496
  garp timer 497
  switchport forbidden vlan 498
  switchport gvrp 499
  show bridge-ext 499
  show garp timer 500
  show gvrp configuration 501

Editing VLAN Groups 501
  vlan database 502
  vlan 502

Configuring VLAN Interfaces 503
  interface vlan 504
  switchport acceptable-frame-types 505
  switchport allowed vlan 506
  switchport ingress-filtering 507
  switchport mode 508
  switchport native vlan 509
  switchport trunk allowed vlan 509
  switchport trunk native vlan 510
  vlan-trunking 511

Displaying VLAN Information 513
show vlan

Configuring IEEE 802.1Q Tunneling
- dot1q-tunnel system-tunnel-control
- dot1q-tunnel tpid
- switchport dot1q-tunnel mode
- switchport dot1q-tunnel service match cvid
- show dot1q-tunnel

Configuring L2CP Tunneling
- l2protocol-tunnel tunnel-dmac
- switchport l2protocol-tunnel
- show l2protocol-tunnel

Configuring Protocol-based VLANs
- protocol-vlan protocol-group (Configuring Groups)
- protocol-vlan protocol-group (Configuring Interfaces)
- show protocol-vlan protocol-group
- show interfaces protocol-vlan protocol-group

Configuring IP Subnet VLANs
- subnet-vlan
- show subnet-vlan

Configuring MAC Based VLANs
- mac-vlan
- show mac-vlan

Configuring Voice VLANs
- voice vlan
- voice vlan aging
- voice vlan mac-address
- switchport voice vlan
- switchport voice vlan priority
- switchport voice vlan rule
- switchport voice vlan security
- show voice vlan

19 Class of Service Commands
Priority Commands (Layer 2)
- queue mode
ip igmp snooping proxy-reporting
ip igmp snooping querier
ip igmp snooping router-alert-option-check
ip igmp snooping router-port-expire-time
ip igmp snooping tcn-flood
ip igmp snooping tcn-query-solicit
ip igmp snooping unregistered-data-flood
ip igmp snooping unsolicited-report-interval
ip igmp snooping version
ip igmp snooping version-exclusive
ip igmp snooping vlan general-query-suppression
ip igmp snooping vlan immediate-leave
ip igmp snooping vlan last-memb-query-count
ip igmp snooping vlan last-memb-query-intvl
ip igmp snooping vlan mrd
ip igmp snooping vlan proxy-address
ip igmp snooping vlan query-interval
ip igmp snooping vlan query-resp-intvl
ip igmp snooping vlan static
clear ip igmp snooping groups dynamic
clear ip igmp snooping statistics
show ip igmp snooping
show ip igmp snooping group
show ip igmp snooping mrouter
show ip igmp snooping statistics

Static Multicast Routing

ip igmp snooping vlan mrouter

IGMP Filtering and Throttling

ip igmp filter (Global Configuration)
ip igmp profile
permit, deny
range
ip igmp authentication
ip igmp filter (Interface Configuration)
ip igmp max-groups
ip igmp max-groups action 602
ip igmp query-drop 603
ip multicast-data-drop 603
show ip igmp authentication 604
show ip igmp filter 604
show ip igmp profile 605
show ip igmp query-drop 606
show ip igmp throttle interface 606
show ip multicast-data-drop 607
MLD Snooping 608
ipv6 mld snooping 609
ipv6 mld snooping querier 609
ipv6 mld snooping query-interval 610
ipv6 mld snooping query-max-response-time 611
ipv6 mld snooping proxy-reporting 611
ipv6 mld snooping robustness 612
ipv6 mld snooping router-port-expire-time 612
ipv6 mld snooping unknown-multicast mode 613
ipv6 mld snooping unsolicited-report-interval 613
ipv6 mld snooping version 614
ipv6 mld snooping vlan immediate-leave 615
ipv6 mld snooping vlan mrouter 615
ipv6 mld snooping vlan static 616
clear ipv6 mld snooping groups dynamic 617
clear ipv6 mld snooping statistics 617
show ipv6 mld snooping 618
show ipv6 mld snooping group 618
show ipv6 mld snooping group source-list 619
show ipv6 mld snooping mrouter 620
show ipv6 mld snooping statistics 620
MLD Filtering and Throttling 621
ipv6 mld filter (Global Configuration) 622
ipv6 mld profile 622
permit, deny 623
range 623
22 LLDP Commands

lldp
lldp holdtime-multiplier
lldp med-fast-start-count
lldp notification-interval
lldp refresh-interval
lldp reinit-delay
lldp tx-delay
lldp admin-status
lldp basic-tlv management-ip-address
lldp basic-tlv port-description
lldp basic-tlv system-capabilities
lldp basic-tlv system-description
lldp basic-tlv system-name
lldp dot1-tlv proto-ident 682
lldp dot1-tlv proto-vid 682
lldp dot1-tlv pvid 683
lldp dot1-tlv vlan-name 683
lldp dot3-tlv link-agg 684
lldp dot3-tlv mac-phy 684
lldp dot3-tlv max-frame 685
lldp dot3-tlv poe 685
lldp med-location civic-addr 686
lldp med-notification 688
lldp med-tlv ext-poe 688
lldp med-tlv inventory 689
lldp med-tlv location 689
lldp med-tlv med-cap 690
lldp med-tlv network-policy 690
lldp notification 691
show lldp config 692
show lldp info local-device 693
show lldp info remote-device 694
show lldp info statistics 695
show lldp neighbors 696

23 CDP Commands 699

    cdp (Global Configuration) 700
    cdp hold-time 700
    cdp transmit-interval 701
    cdp version 701
    cdp (Interface Configuration) 702
    clear cdp table 702
    show cdp 702
    show cdp interface 703
    show cdp neighbors 703

24 Domain Name Service Commands 705

    ip domain-list 705
    ip domain-lookup 706
25 DHCP Commands

DHCP Client

DHCP for IPv4
- ip dhcp client class-id
- ip dhcp restart client

DHCP for IPv6
- ipv6 dhcp client rapid-commit vlan
- ipv6 dhcp restart client vlan
- show ipv6 dhcp duid
- show ipv6 dhcp vlan

DHCP Relay
- ip dhcp relay server
- ip dhcp restart relay

26 IP Interface Commands

IPv4 Interface

Basic IPv4 Configuration
- ip address
- ip default-gateway
- show ip interface
- show ip traffic
- traceroute
- ping

ARP Configuration
- arp
- ip proxy-arp
clear arp-cache 733
show arp 733

IPv6 Interface 734

Interface Address Configuration and Utilities 735
ipv6 default-gateway 735
ipv6 address 736
ipv6 address autoconfig 737
ipv6 address eui-64 739
ipv6 address link-local 741
ipv6 enable 742
ipv6 mtu 743
show ipv6 default-gateway 744
show ipv6 interface 745
show ipv6 mtu 747
show ipv6 traffic 747
traceroute6 752
clear ipv6 traffic 753
ping6 753

Neighbor Discovery 755
ipv6 nd dad attempts 755
ipv6 nd ns-interval 756
ipv6 nd raguard 757
ipv6 nd reachable-time 758
clear ipv6 neighbors 759
show ipv6 nd raguard 759
show ipv6 neighbors 760

ND Snooping 761
ipv6 nd snooping 762
ipv6 nd snooping auto-detect 764
ipv6 nd snooping auto-detect retransmit count 764
ipv6 nd snooping auto-detect retransmit interval 765
ipv6 nd snooping prefix timeout 766
ipv6 nd snooping max-binding 766
ipv6 nd snooping trust 767
clear ipv6 nd snooping binding 767
clear ipv6 nd snooping prefix 768
show ipv6 nd snooping 768
show ipv6 nd snooping binding 769
show ipv6 nd snooping prefix 769

26 IP Routing Commands 771
Global Routing Configuration 771
IPv4 Commands 772
ip route 772
ip sw-route 772
show ip route 773
show ip route database 774
show ip route summary 775

Section III  Appendixes 777

A Troubleshooting 779
Problems Accessing the Management Interface 779
Using System Logs 780

B License Information 781
The GNU General Public License 781
GNU Lesser General Public License, version 3.0 784
The BSD License 786
Open Source Software Used 787
ISC License 787

C Customer Support 793
Zebra Support 793
Customer Support Web Site 793
Manuals 793

Glossary 795
Index of CLI Commands 803
Index 811
Figures

Figure 1: Storm Control by Limiting the Traffic Rate 440
Figure 2: Storm Control by Shutting Down a Port 441
Figure 3: Configuring VLAN Trunking 512
Figure 4: Mapping QinQ Service VLAN to Customer VLAN 519
Tables

Table 1: Options 60, 66 and 67 Statements 70
Table 2: Options 55 and 124 Statements 70
Table 3: General Command Modes 82
Table 4: Configuration Command Modes 84
Table 5: Keystroke Commands 85
Table 6: Command Group Index 86
Table 7: General Commands 89
Table 8: System Management Commands 97
Table 9: Device Designation Commands 97
Table 10: System Status Commands 98
Table 11: show system – display description 103
Table 12: show version – display description 106
Table 13: Frame Size Commands 107
Table 14: Flash/File Commands 109
Table 15: File Directory Information 114
Table 16: Line Commands 120
Table 17: Event Logging Commands 131
Table 18: Logging Levels 132
Table 19: show logging flash/ram - display description 137
Table 20: show logging trap - display description 137
Table 21: Event Logging Commands 138
Table 22: Time Commands 141
Table 23: Predefined Summer-Time Parameters 151
Table 24: Time Range Commands 155
Table 25: Switch Cluster Commands 158
Table 26: Switch Cluster Commands 165
Table 27: SNMP Commands 171
Table 28: show snmp engine-id - display description 186
Table 29: show snmp group - display description 187
| Table 30: show snmp user - display description | 188 |
| Table 31: show snmp view - display description | 189 |
| Table 32: RMON Commands | 195 |
| Table 33: Authentication Commands | 203 |
| Table 34: User Access Commands | 204 |
| Table 35: Default Login Settings | 206 |
| Table 36: Authentication Sequence Commands | 208 |
| Table 37: RADIUS Client Commands | 210 |
| Table 38: TACACS+ Client Commands | 214 |
| Table 39: AAA Commands | 218 |
| Table 40: Web Server Commands | 229 |
| Table 41: HTTPS System Support | 231 |
| Table 42: Telnet Server Commands | 232 |
| Table 43: Secure Shell Commands | 235 |
| Table 44: show ssh - display description | 244 |
| Table 45: 802.1X Port Authentication Commands | 244 |
| Table 46: Management IP Filter Commands | 260 |
| Table 47: PPPoE Intermediate Agent Commands | 262 |
| Table 48: show pppoe intermediate-agent statistics - display description | 269 |
| Table 49: General Security Commands | 271 |
| Table 50: Management IP Filter Commands | 272 |
| Table 51: show port security - display description | 275 |
| Table 52: Network Access Commands | 277 |
| Table 53: Dynamic QoS Profiles | 280 |
| Table 54: Web Authentication | 291 |
| Table 55: DHCP Snooping Commands | 296 |
| Table 56: Option 82 information | 305 |
| Table 57: DHCP Snooping Commands | 309 |
| Table 58: IP Source Guard Commands | 319 |
| Table 59: IPv6 Source Guard Commands | 326 |
| Table 60: ARP Inspection Commands | 332 |
| Table 61: DoS Protection Commands | 340 |
| Table 62: Commands for Configuring Traffic Segmentation | 346 |
| Table 63: Traffic Segmentation Forwarding | 347 |
| Table 64: Access Control List Commands | 351 |
Table 65: IPv4 ACL Commands 351
Table 66: IPv6 ACL Commands 358
Table 67: MAC ACL Commands 364
Table 68: ARP ACL Commands 370
Table 69: ACL Information Commands 373
Table 70: Interface Commands 377
Table 71: show interfaces switchport - display description 390
Table 72: Link Aggregation Commands 403
Table 73: show lacp counters - display description 413
Table 74: show lacp internal - display description 413
Table 75: show lacp neighbors - display description 414
Table 76: show lacp sysid - display description 415
Table 77: PoE Commands 417
Table 78: Maximum Number of Ports Providing Simultaneous Power 420
Table 79: PoE Shut Down Sequence 422
Table 80: show power inline status - display description 423
Table 81: Port Mirroring Commands 425
Table 82: Mirror Port Commands 425
Table 83: RSPAN Commands 428
Table 84: Congestion Control Commands 435
Table 85: Rate Limit Commands 435
Table 86: Rate Limit Commands 437
Table 87: ATC Commands 438
Table 88: Loopback Detection Commands 453
Table 89: Address Table Commands 459
Table 90: Spanning Tree Commands 465
Table 91: Recommended STA Path Cost Range 479
Table 92: Default STA Path Costs 479
Table 93: VLAN Commands 495
Table 94: GVRP and Bridge Extension Commands 496
Table 95: show bridge-ext - display description 500
Table 96: Commands for Editing VLAN Groups 501
Table 97: Commands for Configuring VLAN Interfaces 503
Table 98: Commands for Displaying VLAN Information 513
Table 99: 802.1Q Tunneling Commands 514
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>L2 Protocol Tunnel Commands</td>
<td>521</td>
</tr>
<tr>
<td>101</td>
<td>Protocol-based VLAN Commands</td>
<td>525</td>
</tr>
<tr>
<td>102</td>
<td>IP Subnet VLAN Commands</td>
<td>529</td>
</tr>
<tr>
<td>103</td>
<td>MAC Based VLAN Commands</td>
<td>531</td>
</tr>
<tr>
<td>104</td>
<td>Voice VLAN Commands</td>
<td>533</td>
</tr>
<tr>
<td>105</td>
<td>Priority Commands</td>
<td>541</td>
</tr>
<tr>
<td>106</td>
<td>Priority Commands (Layer 2)</td>
<td>541</td>
</tr>
<tr>
<td>107</td>
<td>Priority Commands (Layer 3 and 4)</td>
<td>546</td>
</tr>
<tr>
<td>108</td>
<td>Default Mapping of CoS/CFI to Internal PHB/Drop Precedence</td>
<td>547</td>
</tr>
<tr>
<td>109</td>
<td>Default Mapping of DSCP Values to Internal PHB/Drop Values</td>
<td>548</td>
</tr>
<tr>
<td>110</td>
<td>Mapping Internal Per-hop Behavior to Hardware Queues</td>
<td>549</td>
</tr>
<tr>
<td>111</td>
<td>Quality of Service Commands</td>
<td>553</td>
</tr>
<tr>
<td>112</td>
<td>Multicast Filtering Commands</td>
<td>571</td>
</tr>
<tr>
<td>113</td>
<td>IGMP Snooping Commands</td>
<td>572</td>
</tr>
<tr>
<td>114</td>
<td>show ip igmp snooping statistics input</td>
<td>593</td>
</tr>
<tr>
<td>115</td>
<td>show ip igmp snooping statistics output</td>
<td>593</td>
</tr>
<tr>
<td>116</td>
<td>show ip igmp snooping statistics vlan query</td>
<td>594</td>
</tr>
<tr>
<td>117</td>
<td>Static Multicast Interface Commands</td>
<td>595</td>
</tr>
<tr>
<td>118</td>
<td>IGMP Filtering and Throttling Commands</td>
<td>596</td>
</tr>
<tr>
<td>119</td>
<td>IGMP Authentication RADIUS Attribute Value Pairs</td>
<td>600</td>
</tr>
<tr>
<td>120</td>
<td>MLD Snooping Commands</td>
<td>608</td>
</tr>
<tr>
<td>121</td>
<td>MLD Filtering and Throttling Commands</td>
<td>621</td>
</tr>
<tr>
<td>122</td>
<td>Multicast VLAN Registration for IPv4 Commands</td>
<td>630</td>
</tr>
<tr>
<td>123</td>
<td>show mvr - display description</td>
<td>644</td>
</tr>
<tr>
<td>124</td>
<td>show mvr interface - display description</td>
<td>646</td>
</tr>
<tr>
<td>125</td>
<td>show mvr members - display description</td>
<td>648</td>
</tr>
<tr>
<td>126</td>
<td>show mvr statistics input - display description</td>
<td>649</td>
</tr>
<tr>
<td>127</td>
<td>show mvr statistics output - display description</td>
<td>650</td>
</tr>
<tr>
<td>128</td>
<td>show mvr statistics query - display description</td>
<td>651</td>
</tr>
<tr>
<td>129</td>
<td>show mvr statistics summary interface - display description</td>
<td>651</td>
</tr>
<tr>
<td>130</td>
<td>show mvr statistics summary interface mvr vlan - description</td>
<td>653</td>
</tr>
<tr>
<td>131</td>
<td>Multicast VLAN Registration for IPv6 Commands</td>
<td>654</td>
</tr>
<tr>
<td>132</td>
<td>show mvr6 - display description</td>
<td>667</td>
</tr>
<tr>
<td>133</td>
<td>show mvr6 interface - display description</td>
<td>668</td>
</tr>
<tr>
<td>134</td>
<td>show mvr6 members - display description</td>
<td>670</td>
</tr>
</tbody>
</table>
Table 135: show mvr6 statistics input - display description 671
Table 136: show mvr6 statistics output - display description 672
Table 137: LLDP Commands 673
Table 138: LLDP MED Location CA Types 687
Table 139: CDP Commands 699
Table 140: show cdp neighbors - display description 704
Table 141: Address Table Commands 705
Table 142: show dns cache - display description 711
Table 143: show hosts - display description 712
Table 144: DHCP Commands 713
Table 145: DHCP Client Commands 713
Table 146: Options 60, 66 and 67 Statements 714
Table 147: Options 55 and 124 Statements 715
Table 148: DHCP Relay Option 82 Commands 719
Table 149: IP Interface Commands 723
Table 150: IPv4 Interface Commands 723
Table 151: Basic IP Configuration Commands 724
Table 152: Address Resolution Protocol Commands 731
Table 153: IPv6 Configuration Commands 734
Table 154: show ipv6 interface - display description 746
Table 155: show ipv6 mtu - display description 747
Table 156: show ipv6 traffic - display description 749
Table 157: show ipv6 neighbors - display description 760
Table 158: ND Snooping Commands 762
Table 203: IP Routing Commands 771
Table 204: Global Routing Configuration Commands 771
Table 205: Troubleshooting Chart 779
Section I

Getting Started

This section describes how to configure the switch for management access through the web interface or SNMP.

This section includes these chapters:

◆ "Initial Switch Configuration" on page 51
Initial Switch Configuration

This chapter includes information on connecting to the switch and basic configuration procedures.

Connecting to the Switch

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see “Setting an IP Address” on page 55.

Configuration Options

The switch’s HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions. The switch’s web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software.

The switch’s web interface, console interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1X security or static address filtering
Connecting to the Console Port

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.

2. Connect the other end of the cable to the RS-45 serial port on the switch.

3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set the baud rate to 115200 bps.
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.
4. Power on the switch.
   After the system completes the boot cycle, the logon screen appears.

For a description of how to use the CLI, see “Using the Command Line Interface” on page 77. For a list of all the CLI commands and detailed information on using the CLI, refer to “CLI Command Groups” on page 86.

Logging Onto the Command Line Interface

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the User name prompt, enter “admin.”
3. At the Password prompt, enter “admin123.” (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 32 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name “admin” and password “admin123” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 password,” for the Normal Exec level, where password is your new password. Press <Enter>. 

– 53 –
4. Type “username admin password 0 password,” for the Privileged Exec level, where password is your new password. Press <Enter>.

Username: admin
Password:

CLI session with the EX-3524* is opened.
To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#

* This manual covers both the EX-3524 and EX-3548 Gigabit Ethernet PoE/PoE+ switches. Other than the difference in the number of ports, there are no other significant differences. Therefore nearly all of the screen display examples are based on the EX-3524.

**Remote Connections**

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IPv4 or IPv6 address.

The default network interface is VLAN 1 which includes ports 1-28/52. When configuring the network interface, the IP address, subnet mask, and default gateway may all be set using a console connection, or DHCP protocol as described in the following sections.

An IPv4 address for the switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see “Setting an IP Address” on page 55.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet or SSH from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions), or from a network computer using SNMP network management software.

**Note:** This switch supports eight Telnet sessions or SSH sessions.

**Note:** Any VLAN group can be assigned an IP interface address (page 72) for managing the switch.

The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.
Configuring the Switch for Remote Management

Using the Network Interface
The switch can be managed through the operational network, known as in-band management. Because in-band management traffic is mixed in with operational network traffic, it is subject to all of the filtering rules usually applied to a standard network ports such as ACLs and VLAN tagging. In-band network management can be accessed via a connection to any network port (1-28/52).

Setting an IP Address
You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

◆ **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

◆ **Dynamic** — The switch can send IPv4 configuration requests to BOOTP or DHCP address allocation servers on the network, or automatically generate a unique IPv6 host address based on the local subnet address prefix received in router advertisement messages. An IPv6 link local address for use in a local network can also be dynamically generated as described in “Obtaining an IPv6 Address” on page 59.

The current software supports DHCP for IPv6, so an IPv6 global unicast address for use in a network containing more than one subnet can be obtained through the DHCPv6 server, or manually configured as described in “Assigning an IPv6 Address” on page 56.

Manual Configuration
You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

**Note:** The IPv4 address for VLAN 1 is obtained via DHCP by default.

Assigning an IPv4 Address
Before you can assign an IPv4 address to the switch, you must obtain the following information from your network administrator:

◆ IP address for the switch
◆ Network mask for this network
◆ Default gateway for the network
To assign an IPv4 address to the switch, complete the following steps

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. Type “ip address ip-address netmask,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.

3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.

4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway gateway,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
```

Assigning an IPv6 Address

This section describes how to configure a “link local” address for connectivity within the local subnet only, and also how to configure a “global unicast” address, including a network prefix for use on a multi-segment network and the host portion of the address.

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see “IPv6 Interface” on page 734.

Link Local Address — All link-local addresses must be configured with a prefix in the range of FE80~FEBF. Remember that this address type makes the switch accessible over IPv6 for all devices attached to the same local subnet only. Also, if the switch detects that the address you configured conflicts with that in use by another device on the subnet, it will stop using the address in question, and automatically generate a link local address that does not conflict with any other devices on the local subnet.

To configure an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. Type “ipv6 address” followed by up to 8 colon-separated 16-bit hexadecimal values for the ipv6-address similar to that shown in the example, followed by the “link-local” command parameter. Then press <Enter>.
Address for Multi-segment Network — Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

◆ Prefix for this network
◆ IP address for the switch
◆ Default gateway for the network

For networks that encompass several different subnets, you must define the full address, including a network prefix and the host address for the switch. You can specify either the full IPv6 address, or the IPv6 address and prefix length. The prefix length for an IPv6 network is the number of bits (from the left) of the prefix that form the network address, and is expressed as a decimal number. For example, all IPv6 addresses that start with the first byte of 73 (hexadecimal) could be expressed as 73:0:0:0:0:0:0:0/8 or 73::/8.

To generate an IPv6 global unicast address for the switch, complete the following steps:

1. From the global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. From the interface prompt, type “ipv6 address ipv6-address” or “ipv6 address ipv6-address/prefix-length,” where “prefix-length” indicates the address bits used to form the network portion of the address. (The network address starts from the left of the prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.

3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type "ipv6 default-gateway gateway," where "gateway" is the IPv6 address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::66/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)#end
```

```
Console#show ipv6 interface
Link-local address:
  fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
  2001:db8:2222:7272::66/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
  ff02::1:ff00:66
  ff02::1:ff11:6700
  ff02::1
IPV6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

```
Console#show ipv6 default-gateway
IPv6 default gateway 2001:db8:2222:7272::254
Console#
```

**Dynamic Configuration**

**Obtaining an IPv4 Address**

If you select the “bootp” or “dhcp” option, the system will immediately start broadcasting service requests. IP will be enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway. If the DHCP/BOOTP server is slow to respond, you may need to use the “ip dhcp restart client” command to re-start broadcasting service requests.

Note that the “ip dhcp restart client” command can also be used to start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. It may be necessary to use this command when DHCP is configured on a VLAN, and the member ports which were previously shut down are now enabled.

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.
To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. At the interface-configuration mode prompt, use one of the following commands:
   - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
   - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.

3. Type “end” to return to the Privileged Exec mode. Press <Enter>.

4. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

5. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

Obtaining an IPv6 Address

Link Local Address — There are several ways to configure IPv6 addresses. The simplest method is to automatically generate a “link local” address (identified by an address prefix in the range of FE80~FEBF). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

To generate an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. Type “ipv6 enable” and press <Enter>.
Address for Multi-segment Network — To generate an IPv6 address that can be used in a network containing more than one subnet, the switch can be configured to automatically generate a unique host address based on the local subnet address prefix received in router advertisement messages. (DHCP for IPv6 can also be used to obtain a unique IPv6 host address.)

To dynamically generate an IPv6 host address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. From the interface prompt, type “ipv6 address autoconfig” and press <Enter>.

3. Type “ipv6 enable” and press <Enter> to enable IPv6 on an interface that has not been configured with an explicit IPv6 address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console(config-if)#ipv6 address autoconfig
Console(config-if)#ipv6 enable
Console(config-if)#end
Console(config)#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
   fe80::2e0:cff:fe00:fd%1/64
Global unicast address(es):
   None
Joined group address(es):
   ff02::1:ff00:fd
   ff02::1
   IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#

---

**Enabling SNMP Management Access**

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to respond to SNMP requests or generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see `snmp-server view` command).

**Community Strings (for SNMP version 1 and 2c clients)**

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.

- **private** - with read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.
To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community string mode,” where “string” is the community access string and “mode” is rw (read/write) or ro (read only). Press <Enter>. (Note that the default mode is read only.)

2. To remove an existing string, simply type “no snmp-server community string;” where “string” is the community access string to remove. Press <Enter>.

| Console(config)#snmp-server community admin rw
| Console(config)#snmp-server community private
| Console(config)# |

**Note:** If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

---

### Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the “snmp-server host” command. From the Privileged Exec level global configuration mode prompt, type:

```
“snmp-server host host-address community-string [version {1 | 2c | 3 [auth | noauth | priv]}]”
```

where “host-address” is the IP address for the trap receiver, “community-string” specifies access rights for a version 1/2c host, or is the user name of a version 3 host, “version” indicates the SNMP client version, and “auth | noauth | priv” means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see the **snmp-server host** command. The following example creates a trap host for each type of SNMP client.

| Console(config)#snmp-server host 10.1.19.23 batman
| Console(config)#snmp-server host 10.1.19.98 robin version 2c
| Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
| Console(config)# |
Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called "mib-2" that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call "r&d" and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth read mib-2 write 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to “Simple Network Management Protocol” in the System Reference Guide, or refer to the specific CLI commands for SNMP starting on page 171 in this guide.

Managing System Files

The switch’s flash memory supports three types of system files that can be managed by the CLI program, the web interface, or SNMP. The switch’s file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via FTP/TFTP to a server for backup. The file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the switch will also create a file named “startup1.cfg” that contains system settings for switch initialization, including information about the unit identifier, and MAC address for the switch. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See “Saving or Restoring Configuration Settings” on page 65 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces.
Diagnostic Code — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Note: The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 32 Mbytes of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Upgrading the Operation Code

The following example shows how to download new firmware to the switch and activate it. The TFTP server could be any standards-compliant server running on Windows or Linux. When downloading from an FTP server, the logon interface will prompt for a user name and password configured on the remote server. Note that “anonymous” is set as the default user name.

File names on the switch are case-sensitive. The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, \, ",")

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
1. config: 2. opcode: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode: m360.bix
Console(config)#exit
Console#dir
File Name                  Type  Startup Modify Time         Size(bytes)
-------------------------- -------------- ------- ------------------- ----------
Unit 1:
m360.bix                        OpCode     Y    2013-02-25 15:41:04   25812529
Factory_Default_Config.cfg       Config     N    2012-12-04 13:18:37        455
startup1.cfg                     Config     Y    2013-03-21 05:39:15       3463
```
Saving or Restoring Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, "", ",", " ")

There can be more than one user-defined configuration file saved in the switch's flash memory, but only one is designated as the “startup” file that is loaded when the switch boots. The `copy running-config startup-config` command always sets the new file as the startup file. To select a previously saved configuration file, use the `boot system config:<filename>` command.

The maximum number of saved configuration files depends on available flash memory. The amount of available flash memory can be checked by using the `dir` command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```console
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.
\Write to FLASH finish.
Success.
Console#
```

To restore configuration settings from a backup server, enter the following command:

1. From the Privileged Exec mode prompt, type “copy tftp startup-config” and press <Enter>.

2. Enter the address of the TFTP server. Press <Enter>.

3. Enter the name of the startup file stored on the server. Press <Enter>.
4. Enter the name for the startup file on the switch. Press <Enter>.

```
Console#copy file startup-config
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:
Success.
Console#
```

Automatic Installation of Operation Code and Configuration Settings

**Downloading Operation Code from a File Server**

Automatic Operation Code Upgrade can automatically download an operation code file when a file newer than the currently installed one is discovered on the file server. After the file is transferred from the server and successfully written to the file system, it is automatically set as the startup file, and the switch is rebooted.

**Usage Guidelines**

- If this feature is enabled, the switch searches the defined URL once during the bootup sequence.

- FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.

- The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

- The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the “/” to indicate this (e.g., ftp://192.168.0.1/).

- The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be ECS4620-28T.bix (using lower case letters as indicated).

- The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some firewalls, even if FTP traffic is not blocked. PASV mode cannot be disabled.

- The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept EX3524_Op.BIX from the server even though EX3524_Op.bix was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unix-like systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are
case-sensitive, meaning that two files in the same directory, `ex3524_op.bix` and `EX3524_Op.BIX` are considered to be unique files. Thus, if the upgrade file is stored as `EX3524_Op.BIX` (or even `Ex3524_Op.bix`) on a case-sensitive server, then the switch (requesting `EX3524_Op.BIX`) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

- Note that the switch itself does not distinguish between upper and lower-case file names, and only checks to see if the file stored on the server is more recent than the current runtime image.

- If two operation code image files are already stored on the switch's file system, then the non-startup image is deleted before the upgrade image is transferred.

- The automatic upgrade process will take place in the background without impeding normal operations (data switching, etc.) of the switch.

- During the automatic search and transfer process, the administrator cannot transfer or update another operation code image, configuration file, public key, or HTTPS certificate (i.e., no other concurrent file management operations are possible).

- The upgrade operation code image is set as the startup image after it has been successfully written to the file system.

- The switch will send an SNMP trap and make a log entry upon all upgrade successes and failures.

- The switch will immediately restart after the upgrade file is successfully written to the file system and set as the startup image.

To enable automatic upgrade, enter the following commands:

1. Specify the TFTP or FTP server to check for new operation code.

   - When specifying a TFTP server, the following syntax must be used, where `filedir` indicates the path to the directory containing the new image:
     
     `tftp://192.168.0.1[/filedir]/`

   - When specifying an FTP server, the following syntax must be used, where `filedir` indicates the path to the directory containing the new image:
     
     `ftp://[username[:password@]]192.168.0.1[/filedir]/`

     If the user name is omitted, “anonymous” will be used for the connection. If the password is omitted a null string (""") will be used for the connection.
This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://zebra:billy@192.168.0.1/sm24/
Console(config)#
```

2. Set the switch to automatically reboot and load the new code after the opcode upgrade is completed.

```
Console(config)#upgrade opcode reload
Console(config)#
```

3. Set the switch to automatically upgrade the current operational code when a new version is detected on the server. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:

   a. It will search for a new version of the image at the location specified by `upgrade opcode path` command. The name for the new image stored on the TFTP server must be EX3524_Op.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.

   b. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.

   c. It sets the new version as the startup image.

   d. It then restarts the system to start using the new image.

```
Console(config)#upgrade opcode auto
Console(config)#
```

4. Display the automatic upgrade settings.

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status       : Enabled
  Reload Status : Enabled
  Path         :
  File Name    : EX3524_Op.bix
Console#
```
Specifying a DHCP Client Identifier

DHCP servers index their database of address bindings using the client’s Media Access Control (MAC) Address or a unique client identifier. The client identifier is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.

DHCP client Identifier (Option 60) is used by DHCP clients to specify their unique identifier. The client identifier is optional and can be specified while configuring DHCP on the primary network interface. DHCP Option 60 is disabled by default.

The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60 (vendor-class-identifier), 66 (tftp-server-name) and 67 (bootfile-name) statements can be added to the server daemon’s configuration file as described in the following section.

If the DHCP server has an index entry for a switch requesting service, it should reply with the TFTP server name and boot file name. Note that the vendor class identifier can be formatted in either text or hexadecimal, but the format used by both the client and server must be the same.

```bash
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

Downloading a Configuration File Referred by a DHCP Server

Information passed on to the switch from a DHCP server may also include a configuration file to be downloaded and the TFTP servers where that file can be accessed. If the Factory Default Configuration file is used to provision the switch at startup, in addition to requesting IP configuration settings from the DHCP server, it will also ask for the name of a bootup configuration file and TFTP servers where that file is stored.

If the switch receives information that allows it to download the remote bootup file, it will save this file to a local buffer, and then restart the provision process.

Note the following DHCP client behavior:

- The bootup configuration file received from a TFTP server is stored on the switch with the original file name. If this file name already exists in the switch, the file is overwritten.

- If the name of the bootup configuration file is the same as the Factory Default Configuration file, the download procedure will be terminated, and the switch will not send any further DHCP client requests.
◆ If the switch fails to download the bootup configuration file based on information passed by the DHCP server, it will not send any further DHCP client requests.

◆ If the switch does not receive a DHCP response prior to completing the bootup process, it will continue to send a DHCP client request once a minute. These requests will only be terminated if the switch’s address is manually configured, but will resume if the address mode is set back to DHCP.

To successfully transmit a bootup configuration file to the switch, the DHCP daemon (using a Linux based system for this example) must be configured with the following information:

◆ Options 60, 66 and 67 statements can be added to the daemon’s configuration file.

Table 1: Options 60, 66 and 67 Statements

<table>
<thead>
<tr>
<th>Option</th>
<th>Keyword</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>vendor-class-identifier</td>
<td>a string indicating the vendor class identifier</td>
</tr>
<tr>
<td>66</td>
<td>tftp-server-name</td>
<td>a string indicating the tftp server name</td>
</tr>
<tr>
<td>67</td>
<td>bootfile-name</td>
<td>a string indicating the bootfile name</td>
</tr>
</tbody>
</table>

◆ By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a “parameter request list” asking for this information. Besides these items, the client request also includes a “vendor class identifier” that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 2: Options 55 and 124 Statements

<table>
<thead>
<tr>
<th>Option</th>
<th>Keyword</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>dhcp-parameter-request-list</td>
<td>a list of parameters, separated by a comma ','</td>
</tr>
<tr>
<td>124</td>
<td>vendor-class-identifier</td>
<td>a string indicating the vendor class identifier</td>
</tr>
</tbody>
</table>

The following configuration example is provided for a Linux-based DHCP daemon (dhcpd.conf file). In the “Vendor class” section, the server will always send Option 66 and 67 to tell the switch to download the “test” configuration file from server 192.168.255.101.

```
ddns-update-style ad-hoc;

default-lease-time 600;
max-lease-time 7200;
```
log-facility local7;

server-name "Server1";
Server-identifier 192.168.255.250;
#option 66, 67
  option space dynamicProvision code width 1 length 1 hash size 2;
  option dynamicProvision.tftp-server-name code 66 = text;
  option dynamicProvision.bootfile-name code 67 = text;

subnet 192.168.255.0 netmask 255.255.255.0 {
  range 192.168.255.160 192.168.255.200;
  option routers 192.168.255.101;
  option tftp-server-name "192.168.255.100";  #Default Option 66
  option bootfile-name "bootfile";  #Default Option 67
}

class "Option66,67_1" {  #DHCP Option 60 Vendor class two
  match if option vendor-class-identifier = "EX3524_Op.cfg";
  option tftp-server-name "192.168.255.101";
  option bootfile-name "test";
}

Note: Use "EX3524_Op.cfg" for the vendor-class-identifier in the dhcpd.conf file.

---

### Setting the System Clock

Simple Network Time Protocol (SNTP) or Network Time Protocol (NTP) can be used to set the switch's internal clock based on periodic updates from a time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP or NTP, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

The switch also supports the following time settings:

- **Time Zone** – You can specify the offset from Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

- **Summer Time/Daylight Saving Time (DST)** – In some regions, the time shifts by one hour in the fall and spring. The switch supports manual entry for one-time or recurring clock shifts.
Setting the System Clock

To manually set the clock to 14:11:36, April 1st, 2013, enter this command.

```
Console#calendar set 14 11 36 1 April 2013
Console#
```

To set the time zone, enter a command similar to the following.

```
Console(config)#clock timezone Japan hours 8 after-UTC
Console(config)#
```

To set the time shift for summer time, enter a command similar to the following.

```
Console(config)#clock summer-time SUMMER date 2 april 2013 0 0 30 june 2013 0 0
Console(config)#
```

To display the clock configuration settings, enter the following command.

```
Console#show calendar
Current Time          : Apr  2 15:56:12 2013
Time Zone             : UTC, 08:00
Summer Time           : SUMMER, offset 60 minutes
                      : Apr 2 2013 00:00 to Jun 30 2013 00:00
Summer Time in Effect : Yes
Console#
```

Configuring SNTP

Setting the clock based on an SNTP server can provide more accurate clock synchronization across network switches than manually-configured time. To configure SNTP, set the switch as an SNTP client, and then set the polling interval, and specify a time server as shown in the following example.

```
Console(config)#sntp client
Console(config)#sntp poll 60
Console(config)#sntp server 10.1.0.19
Console(config)#exit
Console#show sntp
Current Time   : Apr  2 16:06:07 2013
Poll Interval  : 60 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 10.1.0.19
Current Server : 10.1.0.19
Console#
```
Configuring NTP

Requesting the time from an NTP server is the most secure method. You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

When more than one time server is configured, the client will poll all of the time servers, and compare the responses to determine the most reliable and accurate time update for the switch.

To configure NTP time synchronization, enter commands similar to the following.

```
Console(config)#ntp client
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#ntp authenticate
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#exit

Console#show ntp
Polling : 1024 seconds
Current Mode : unicast
NTP Status : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server : 192.168.0.88 Port: 123
Last Update Time : Mar 12 02:41:01 2013 UTC
NTP Server 192.168.0.88 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885

Current Time : Apr  2 16:28:34 2013
Polling : 1024 seconds
Current Mode : unicast
NTP Status : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server : 192.168.5.23 Port: 0
Last Update Time : Apr  2 16:00:00 2013 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.5.23 version 3 key 19
NTP Authentication Key 45 md5 2662T75S5658RU542418034777

Console#
```
Setting the System Clock
Command Line Interface

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

◆ “General Commands” on page 89
◆ “System Management Commands” on page 97
◆ “SNMP Commands” on page 171
◆ “Remote Monitoring Commands” on page 195
◆ “Authentication Commands” on page 203
◆ “General Security Measures” on page 271
◆ “Access Control Lists” on page 351
◆ “Interface Commands” on page 377
◆ “Link Aggregation Commands” on page 403
◆ “Power over Ethernet Commands” on page 417
◆ “Port Mirroring Commands” on page 425
◆ “Congestion Control Commands” on page 435
◆ “Loopback Detection Commands” on page 453
◆ “Address Table Commands” on page 459
◆ “Spanning Tree Commands” on page 465
◆ “VLAN Commands” on page 495
◆ “Class of Service Commands” on page 541
◆ “Quality of Service Commands” on page 553
◆ “Multicast Filtering Commands” on page 571
◆ “LLDP Commands” on page 673
◆ “CDP Commands” on page 699
◆ “Domain Name Service Commands” on page 705
◆ “DHCP Commands” on page 713
◆ “IP Interface Commands” on page 723
◆ “IP Routing Commands” on page 771
Using the Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server’s console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch’s command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are “admin” and “guest” with corresponding passwords of “admin” and “guest.”) When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

User Access Verification
Username: admin
Password:

CLI session with the EX-3524 is opened.
To end the CLI session, enter [Exit].

Console#
Telnet Connection  
Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.4 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.

2. At the prompt, enter the user name and system password. The CLI will display the “Vty-n#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-n=” for the guest to show that you are using normal access mode (i.e., Normal Exec), where n indicates the number of the current Telnet session.

3. Enter the necessary commands to complete your desired tasks.

4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

CLI session with the EX-3524 is opened.
To end the CLI session, enter [Exit].

Vty-1#
```

Vty-1#
Note: You can open up to eight sessions to the device via Telnet or SSH.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” `show interfaces` and `status` are keywords, `ethernet` is an argument that specifies the interface type, and `1/5` specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter the following commands. The default password “super” is used to change from Normal Exec to Privileged Exec mode.

```
Console> enable
Password:
Console# show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)# username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as `con`. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing `log` followed by a tab will result in printing the command up to “logging.”
Getting Help on Commands

You can display a brief description of the help system by entering the `help` command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command “show ?” displays a list of possible show commands:

```
Console#show ?
access-group       Access groups
access-list        Access lists
accounting         Uses the specified accounting list
adoption           Adoption related information
arp                Information of ARP cache
authorization      Enables EXEC accounting
auto-traffic-control Auto traffic control information
bridge-ext         Bridge extension information
cable-diagnostics  Shows the information of cable diagnostics
calendar           Date and time information
cdp                CDP
class-map          Displays class maps
cluster            Display cluster
collision-mac-address-table Show collision mac address
debug             State of each debugging option
dns                DNS information
dos-protection     Shows the system dos-protection summary information
dot1q-tunnel       dot1q-tunnel
dot1x              802.1X content
garp               GARP properties
gvgrp              GVRP interface information
history            Shows history information
hosts              Host information
interfaces         Shows interface information
ip                 IP information
ipv6               IPv6 information
l2protocol-tunnel  Layer 2 protocol tunneling configuration
lacp               LACP statistics
line               TTY line information
lldp               LLDP
log                Log records
logging            Logging setting
loop               Shows the information of loopback
loopback-detection Shows loopback detection information
mac                MAC access list
mac-address-table  Configuration of the address table
mac-vlan           MAC-based VLAN information
management         Shows management information
memory             Memory utilization
mvr                multicast VLAN registration
mvr6               IPv6 multicast VLAN registration
neighbors          Shows LLDP neighbors information
network-access     Shows the entries of the secure port.
nlm                Show notification log
ntp                Network Time Protocol configuration
policy-map         Displays policy maps
port               Port characteristics
port-channel       Port channel information
```
Console#show interfaces ?

bright                      Shows brief interface description
counters                    Interface counters information
protocol-vlan               Protocol-VLAN information
status                      Shows interface status
switchport                  Shows interface switchport information
transceiver                 Interface of transceiver information
transceiver-threshold       Interface of transceiver-threshold information
Console#

Show commands which display more than one page of information (e.g., `show running-config`) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.
Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “s?” shows all the keywords starting with “s.”

```
Console#show s?
    snmp          snmp-server    sntp          spanning-tree    ssh
    startup-config subnet-vlan    system
Console#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “no” to cancel the effect of a command or reset the configuration to the default value. For example, the `logging` command will log system messages to a host server. To disable logging, specify the `no logging` command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the `show history` command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “?” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

<table>
<thead>
<tr>
<th>Class</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec</td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td>Privileged</td>
</tr>
<tr>
<td>Configuration</td>
<td>Global*</td>
</tr>
</tbody>
</table>

Access Control List
Class Map
IGMP Profile
Interface
Line
Multiple Spanning Tree
Policy Map
Time Range
VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.
You must be in Global Configuration mode to access any of the other configuration modes.
Exec Commands When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name “admin” and password “admin123.” The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the enable command, followed by the privileged level password “super.”

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

CLI session with the EX-3524 is opened.
To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

CLI session with the EX-3524 is opened.
To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

Configuration Commands Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the copy running-config startup-config command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as hostname and snmp-server community.

- Access Control List Configuration - These commands are used for packet filtering.

- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.

- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.

- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.

- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.

- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.

- Time Range - Sets a time range for use by other functions, such as Access Control Lists.

- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command `configure` in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

**Table 4: Configuration Command Modes**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Command</th>
<th>Prompt</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>access-list ip standard</td>
<td>Console(config-std-acl)</td>
<td>352</td>
</tr>
<tr>
<td></td>
<td>access-list ip extended</td>
<td>Console(config-ext-acl)</td>
<td>352</td>
</tr>
<tr>
<td></td>
<td>access-list ipv6 standard</td>
<td>Console(config-std-ipv6-acl)</td>
<td>359</td>
</tr>
<tr>
<td></td>
<td>access-list ipv6 extended</td>
<td>Console(config-ext-ipv6-acl)</td>
<td>360</td>
</tr>
<tr>
<td></td>
<td>access-list mac</td>
<td>Console(config-mac-acl)</td>
<td>364</td>
</tr>
<tr>
<td>Class Map</td>
<td>class-map</td>
<td>Console(config-cmap)</td>
<td>554</td>
</tr>
<tr>
<td>Interface</td>
<td>interface {ethernet port</td>
<td>port-channel id} vlan id}</td>
<td>Console(config-if)</td>
</tr>
<tr>
<td>Line</td>
<td>line {console</td>
<td>vty}</td>
<td>Console(config-line-console)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Console(config-line-vty)</td>
<td>121</td>
</tr>
<tr>
<td>MSTP</td>
<td>spanning-tree mst-configuration</td>
<td>Console(config-mstp)</td>
<td>472</td>
</tr>
<tr>
<td>Policy Map</td>
<td>policy-map</td>
<td>Console(config-pmap)</td>
<td>557</td>
</tr>
<tr>
<td>Time Range</td>
<td>time-range</td>
<td>Console(config-time-range)</td>
<td>155</td>
</tr>
<tr>
<td>VLAN</td>
<td>vlan database</td>
<td>Console(config-vlan)</td>
<td>502</td>
</tr>
</tbody>
</table>
For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode.

```
Console(config)#interface ethernet 1/5
.
Console(config-if)#exit
Console(config)#
```

**Command Line Processing**

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

**Table 5: Keystroke Commands**

<table>
<thead>
<tr>
<th>Keystroke</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-A</td>
<td>Shifts cursor to start of command line.</td>
</tr>
<tr>
<td>Ctrl-B</td>
<td>Shifts cursor to the left one character.</td>
</tr>
<tr>
<td>Ctrl-C</td>
<td>Terminates the current task and displays the command prompt.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Shifts cursor to end of command line.</td>
</tr>
<tr>
<td>Ctrl-F</td>
<td>Shifts cursor to the right one character.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Deletes all characters from the cursor to the end of the line.</td>
</tr>
<tr>
<td>Ctrl-L</td>
<td>Repeats current command line on a new line.</td>
</tr>
<tr>
<td>Ctrl-N</td>
<td>Enters the next command line in the history buffer.</td>
</tr>
<tr>
<td>Ctrl-P</td>
<td>Enters the last command.</td>
</tr>
<tr>
<td>Ctrl-R</td>
<td>Repeats current command line on a new line.</td>
</tr>
<tr>
<td>Ctrl-U</td>
<td>Deletes from the cursor to the beginning of the line.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Deletes the last word typed.</td>
</tr>
<tr>
<td>Esc-B</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc-D</td>
<td>Deletes from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Esc-F</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td>Delete key or backspace key</td>
<td>Erases a mistake when entering a command.</td>
</tr>
</tbody>
</table>
CLI Command Groups

The system commands can be broken down into the functional groups shown below.

Table 6: Command Group Index

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Basic commands for entering privileged access mode, restarting the system, or quitting the CLI</td>
<td>89</td>
</tr>
<tr>
<td>System Management</td>
<td>Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, the system clock, and switch clustering</td>
<td>97</td>
</tr>
<tr>
<td>Simple Network Management Protocol</td>
<td>Activates authentication failure traps; configures community access strings, and trap receivers</td>
<td>171</td>
</tr>
<tr>
<td>Remote Monitoring</td>
<td>Supports statistics, history, alarm and event groups</td>
<td>195</td>
</tr>
<tr>
<td>User Authentication</td>
<td>Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses</td>
<td>203</td>
</tr>
<tr>
<td>General Security Measures</td>
<td>Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses</td>
<td>271</td>
</tr>
<tr>
<td>Access Control List</td>
<td>Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address or DSCP traffic class), or non-IP frames (based on MAC address or Ethernet type)</td>
<td>351</td>
</tr>
<tr>
<td>Interface</td>
<td>Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs</td>
<td>377</td>
</tr>
<tr>
<td>Link Aggregation</td>
<td>Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks</td>
<td>403</td>
</tr>
<tr>
<td>Power over Ethernet</td>
<td>Configures power output for connected devices</td>
<td>417</td>
</tr>
<tr>
<td>Mirror Port</td>
<td>Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port</td>
<td>425</td>
</tr>
<tr>
<td>Congestion Control</td>
<td>Sets the input/output rate limits, traffic storm thresholds, and thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.</td>
<td>435</td>
</tr>
<tr>
<td>Loopback Detection</td>
<td>Detects general loopback conditions caused by hardware problems or faulty protocol settings</td>
<td>453</td>
</tr>
<tr>
<td>Address Table</td>
<td>Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time</td>
<td>459</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>Configures Spanning Tree settings for the switch</td>
<td>465</td>
</tr>
<tr>
<td>VLANs</td>
<td>Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling</td>
<td>495</td>
</tr>
</tbody>
</table>
Table 6: Command Group Index (Continued)

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of Service</td>
<td>Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for DSCP</td>
<td>541</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>Configures Differentiated Services</td>
<td>553</td>
</tr>
<tr>
<td>Multicast Filtering</td>
<td>Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration</td>
<td>571</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol</td>
<td>Configures LLDP settings to enable information discovery about neighbor devices</td>
<td>673</td>
</tr>
<tr>
<td>Cisco Discovery Protocol</td>
<td>Configures CDP settings to enable information discovery about neighbor devices</td>
<td>699</td>
</tr>
<tr>
<td>Domain Name Service</td>
<td>Configures DNS services.</td>
<td>705</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol</td>
<td>Configures DHCP client functions</td>
<td>713</td>
</tr>
<tr>
<td>IP Interface</td>
<td>Configures IP address for the switch interfaces; also configures ARP parameters and static entries</td>
<td>723</td>
</tr>
<tr>
<td>IP Routing</td>
<td>Configures static unicast routing</td>
<td>771</td>
</tr>
</tbody>
</table>

The access mode shown in the following tables is indicated by these abbreviations:

- **ACL** (Access Control List Configuration)
- **CM** (Class Map Configuration)
- **GC** (Global Configuration)
- **IC** (Interface Configuration)
- **IPC** (IGMP Profile Configuration)
- **LC** (Line Configuration)
- **MST** (Multiple Spanning Tree)
- **NE** (Normal Exec)
- **PE** (Privileged Exec)
- **PM** (Policy Map Configuration)
- **VC** (VLAN Database Configuration)
Chapter 2 | Using the Command Line Interface

CLI Command Groups
General Commands

The general commands are used to control the command access mode, configuration mode, and other basic functions.

Table 7: General Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>prompt</td>
<td>Customizes the CLI prompt</td>
<td>GC</td>
</tr>
<tr>
<td>reload</td>
<td>Restarts the system at a specified time, after a specified delay, or at a periodic interval</td>
<td>GC</td>
</tr>
<tr>
<td>enable</td>
<td>Activates privileged mode</td>
<td>NE</td>
</tr>
<tr>
<td>quit</td>
<td>Exits a CLI session</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show history</td>
<td>Shows the command history buffer</td>
<td>NE, PE</td>
</tr>
<tr>
<td>configure</td>
<td>Activates global configuration mode</td>
<td>PE</td>
</tr>
<tr>
<td>disable</td>
<td>Returns to normal mode from privileged mode</td>
<td>PE</td>
</tr>
<tr>
<td>reload</td>
<td>Restarts the system immediately</td>
<td>PE</td>
</tr>
<tr>
<td>show reload</td>
<td>Displays the current reload settings, and the time at which next scheduled reload will take place</td>
<td>PE</td>
</tr>
<tr>
<td>end</td>
<td>Returns to Privileged Exec mode</td>
<td>any config. mode</td>
</tr>
<tr>
<td>exit</td>
<td>Returns to the previous configuration mode, or exits the CLI</td>
<td>any mode</td>
</tr>
<tr>
<td>help</td>
<td>Shows how to use help</td>
<td>any mode</td>
</tr>
<tr>
<td>?</td>
<td>Shows options for command completion (context sensitive)</td>
<td>any mode</td>
</tr>
</tbody>
</table>

**prompt** This command customizes the CLI prompt. Use the no form to restore the default prompt.

**Syntax**

```
prompt string
```

```
no prompt
```

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 32 characters)

**Default Setting**

Console
Command Mode
Global Configuration

Command Usage
This command and the hostname command can be used to set the command line prompt as shown in the example below. Using the no form of either command will restore the default command line prompt.

Example

```
Console(config)#prompt RD2
RD2(config)#
```

reload
(Global Configuration)
This command restarts the system at a specified time, after a specified delay, or at a periodic interval. You can reboot the system immediately, or you can configure the switch to reset after a specified amount of time. Use the cancel option to remove a configured setting.

Syntax

```
reload [at hour minute [(month day | day month) [year]] |
in (hour hours | minute minutes | hour hours minute minutes) |
regularity hour minute [period (daily | monthly day-of-month | weekly day-of-week)] | cancel [at | in | regularity]]
```

**reload at** - A specified time at which to reload the switch.

- **hour** - The hour at which to reload. (Range: 0-23)
- **minute** - The minute at which to reload. (Range: 0-59)
- **month** - The month at which to reload. (january ... december)
- **day** - The day of the month at which to reload. (Range: 1-31)
- **year** - The year at which to reload. (Range: 1970-2037)

**reload in** - An interval after which to reload the switch.

- **hours** - The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)
- **minutes** - The number of minutes, combined with the hours, before the switch resets. (Range: 0-34560)

**reload regularity** - A periodic interval at which to reload the switch.

- **hour** - The hour at which to reload. (Range: 0-23)
- **minute** - The minute at which to reload. (Range: 0-59)
- **day-of-month** - Day of the month at which to reload. (Range: 1-31)
- **day-of-week** - Day of the week at which to reload. (Range: monday ... saturday)

**reload cancel** - Cancels the specified reload option.
Default Setting
None

Command Mode
Global Configuration

Command Usage
◆ This command resets the entire system.

◆ Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.

◆ When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (See “copy” on page 110).

Example
This example shows how to reset the switch after 30 minutes:

```
Console(config)#reload in minute 30
*** --- Rebooting at January 1 02:10:43 2007 ---
***
Are you sure to reboot the system at the specified time? <y/n>
```

enable
This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See “Understanding Command Modes” on page 82.

Syntax
```
enable [level]
```

`level` - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting
Level 15

Command Mode
Normal Exec

Command Usage
◆ “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the enable password command.)
◆ The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

**Example**

```
Console>enable
Password: [privileged level password]
Console#
```

**Related Commands**

- disable (94)
- enable password (204)

**quit**  This command exits the configuration program.

**Default Setting**
None

**Command Mode**
Normal Exec, Privileged Exec

**Command Usage**
The *quit* and *exit* commands can both exit the configuration program.

**Example**
This example shows how to quit a CLI session:

```
Console#quit

% CLI exit session
```

**show history**  This command shows the contents of the command history buffer.

**Default Setting**
None

**Command Mode**
Normal Exec, Privileged Exec

**Command Usage**
The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.
Example
In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
  2 config
  1 show history

Configuration command history:
  4 interface vlan 1
  3 exit
  2 interface vlan 1
  1 end

Console#
```

The ! command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the !2 command repeats the second command in the Execution history buffer (config).

```
Console#!2
Console#config
Console(config)#
```

configure
This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration. See “Understanding Command Modes” on page 82.

Default Setting
None

Command Mode
Privileged Exec

Example
```
Console#configure
Console(config)#
```

Related Commands
der (95)
disable  This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See “Understanding Command Modes” on page 82.

Default Setting
None

Command Mode
Privileged Exec

Command Usage
The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example
```
Console#disable
Console>
```

Related Commands
enable (91)

reload (Privileged Exec)  This command restarts the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

Default Setting
None

Command Mode
Privileged Exec

Command Usage
This command resets the entire system.

Example
This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```
**show reload**  This command displays the current reload settings, and the time at which next scheduled reload will take place.

**Command Mode**
Privileged Exec

**Example**

```
Console#show reload
Reloading switch in time: 0 hours 29 minutes.
The switch will be rebooted at January 1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

**end**  This command returns to Privileged Exec mode.

**Default Setting**
None

**Command Mode**
Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

**Example**

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

**exit**  This command returns to the previous configuration mode or exits the configuration program.

**Default Setting**
None

**Command Mode**
Any
Example
This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
% CLI exit session
```

Press ENTER to start session
System Management Commands

The system management commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 8: System Management Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Designation</td>
<td>Configures information that uniquely identifies this switch</td>
</tr>
<tr>
<td>System Status</td>
<td>Displays system configuration, active managers, and version information</td>
</tr>
<tr>
<td>Frame Size</td>
<td>Enables support for jumbo frames</td>
</tr>
<tr>
<td>File Management</td>
<td>Manages code image or switch configuration files</td>
</tr>
<tr>
<td>Line</td>
<td>Sets communication parameters for the serial port, including baud rate and console time-out</td>
</tr>
<tr>
<td>Event Logging</td>
<td>Controls logging of error messages</td>
</tr>
<tr>
<td>SMTP Alerts</td>
<td>Configures SMTP email alerts</td>
</tr>
<tr>
<td>Time (System Clock)</td>
<td>Sets the system clock automatically via NTP/SNTP server or manually</td>
</tr>
<tr>
<td>Time Range</td>
<td>Sets a time range for use by other functions, such as Access Control Lists</td>
</tr>
<tr>
<td>Switch Clustering</td>
<td>Configures management of multiple devices via a single IP address</td>
</tr>
<tr>
<td>Adopt Device</td>
<td>Configures switch to submit request to be adopted for centralized management by “Controller” software</td>
</tr>
</tbody>
</table>

Device Designation

This section describes commands used to configure information that uniquely identifies the switch.

Table 9: Device Designation Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Specifies the host name for the switch</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server contact</td>
<td>Sets the system contact string</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server location</td>
<td>Sets the system location string</td>
<td>GC</td>
</tr>
</tbody>
</table>
**hostname**  This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

**Syntax**

```
hostname name
no hostname
```

`name` - The name of this host. (Maximum length: 255 characters)

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- The host name specified by this command is displayed by the `show system` command and on the Show > System web page.
- This command and the `prompt` command can be used to set the command line prompt as shown in the example below. Using the **no** form of either command will restore the default command line prompt.

**Example**

```
Console(config)#hostname RD#1
RD#1(config)#
```

---

**System Status**

This section describes commands used to display system information.

**Table 10: System Status Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-list</td>
<td>Shows utilization parameters for TCAM</td>
<td>PE</td>
</tr>
<tr>
<td>tcam-utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show memory</td>
<td>Shows memory utilization parameters</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show process cpu</td>
<td>Shows CPU utilization parameters</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the configuration data currently in use</td>
<td>PE</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the contents of the configuration file (stored in flash memory) that is used to start up the system</td>
<td>PE</td>
</tr>
<tr>
<td>show system</td>
<td>Displays system information</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show tech-support</td>
<td>Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems</td>
<td>PE</td>
</tr>
</tbody>
</table>
show access-list tcam-utilization

This command shows utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries.

**Command Mode**
Privileged Exec

**Command Usage**
Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

**Example**

```
Console#show access-list tcam-utilization
Pool capability code:
    ALL - All supported function, AM - MAC ACL, A4 - IPv4 ACL,
    A6S - IPv6 Standard ACL, A6E - IPv6 extended ACL, DM - MAC DiffServ,
    D4 - IPv4 DiffServ, D6S - IPv6 standard DiffServ,
    D6E - IPv6 extended DiffServ, AEM - Egress MAC ACL,
    AE4 - Egress IPv4 ACL, AE6S - Egress IPv6 standard ACL,
    AE6E - Egress IPv6 extended ACL, DEM - Egress MAC DiffServ,
    DE4 - Egress IPv4 DiffServ, DE6S - Egress IPv6 standard DiffServ,
    DE6E - Egress IPv6 extended DiffServ, W - Web authentication,
    I - IP source guard, I6 - IPv6 source guard, C - CPU interface,
    R - Rate limit, L - Link local, Reserved - Reserved

Unit  Device  Pool  Total  Used  Free  Pool  Capability
       ---  ------  -----  -----  -----  ------  ---------------------------
        1      0      0    372    196   176  ALL
        1      1      0    372    196   176  ALL

Console#
```
**show memory**  This command shows memory utilization parameters.

**Command Mode**
Normal Exec, Privileged Exec

**Command Usage**
This command shows the amount of memory currently free for use, the amount of memory allocated to active processes, the total amount of system memory, and the alarm thresholds.

**Example**

```
Console#show memory
Status Bytes      %
------ ---------- ---
Free     19951616  14
Used    114266112  86
Total   134217728

Alarm Configuration
Rising Threshold : 95%
Falling Threshold : 90%
```

**Related Commands**
memory (192)

**show process cpu**  This command shows the CPU utilization parameters, alarm status, and alarm thresholds.

**Command Mode**
Normal Exec, Privileged Exec

**Example**

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 22%

CPU Utilization in the past 60 seconds
Average Utilization : 27%
Maximum Utilization : 39%

Alarm Status
Current Alarm Status : Off
Last Alarm Start Time :
Last Alarm Duration Time : 44 seconds

Alarm Configuration
Rising Threshold : 90%
Falling Threshold : 70%
```

Console#
show running-config  This command displays the configuration information currently in use.

Syntax

show running-config [interface interface]

interface

ethernet unit/port

unit - Unit identifier. (Range: Always 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)

vlan vlan-id (Range: 1-4094)

Command Mode
Privileged Exec

Command Usage
◆ Use the interface keyword to display configuration data for the specified interface.

◆ Use this command in conjunction with the show startup-config command to compare the information in running memory to the information stored in non-volatile memory.

◆ This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

- MAC address for the switch
- SNMP community strings
- Users (names, access levels, and encrypted passwords)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for management VLAN
- Spanning tree settings
- Interface settings
- Any configured settings for the console port and Telnet

Example

```
Console#show running-config
Building running configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_03</stackingMac>
!
```
snmp-server community public ro
snmp-server community private rw

! snmp-server enable traps authentication

!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
enable password level 15 7 b3231655cebb7a1f783edd27d254ca

!
vlan database
  vlan 1 name DefaultVlan media ethernet state active
  spanning-tree mst configuration
  !
  interface ethernet 1/1
  !
  interface ethernet 1/1
  ip address dhcp
  :
  radius-server acct-port 1813
  :
  interface vlan 1
  ip address 192.168.1.10 255.255.255.0

!
  line console
  !
  line vty
  !
  end
  !
  Console#

---

**Related Commands**

**show startup-config** (102)

**show startup-config**  This command displays the configuration file stored in non-volatile memory that is used to start up the system.

**Command Mode**

Privileged Exec

**Command Usage**

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.

- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for the switch
  - SNMP community strings
  - SNMP trap authentication
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
Multiple spanning tree instances (name and interfaces)
- Interface settings and VLAN configuration settings for each interface
- IP address for management VLAN
- Any configured settings for the console port and Telnet

Example
Refer to the example for the running configuration file.

Related Commands
show running-config (101)

show system This command displays system information.

Default Setting
None

Command Mode
Normal Exec, Privileged Exec

- The number of fans provided: EX-3524 - 2, EX-3548 - 3
- The EX-3528 does not monitor system temperature.

Example

```
Console#show system
System Description : EX-3524 Managed POE/POE+ Switch
System OID String  : 1.3.6.1.4.1.388.19.101
System Information
  System Up Time       : 0 days, 5 hours, 48 minutes, and 23.9 seconds
  System Name          :
  System Location      :
  System Contact       :
  MAC Address (Unit 1) : FC-0A-81-B7-C7-E0
  Web Server           : Enabled
  Web Server Port      : 80
  Web Secure Server    : Enabled
  Web Secure Server Port : 443
  Telnet Server        : Enabled
  Telnet Server Port   : 23
  Jumbo Frame          : Disabled
Unit 1
  Fan 1: Ok           Fan 2: Ok

Console#
```

Table 11: show system – display description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Description</td>
<td>Brief description of device type.</td>
</tr>
<tr>
<td>System OID String</td>
<td>MIB II object ID for switch's network management subsystem.</td>
</tr>
</tbody>
</table>
**show tech-support**

This command displays a detailed list of system settings designed to help technical support resolve configuration or functional problems.

**Command Mode**

Normal Exec, Privileged Exec

**Command Usage**

This command generates a long list of information including detailed system and interface settings. It is therefore advisable to direct the output to a file using any suitable output capture function provided with your terminal emulation program.

**Example**

```
Console#show tech-support

dir:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Type</th>
<th>Startup</th>
<th>Modify Time</th>
<th>Size(bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory_Default_Config.cfg</td>
<td>Config</td>
<td>N</td>
<td>2014-08-24 06:40:02</td>
<td>455</td>
</tr>
<tr>
<td>startup1.cfg</td>
<td>Config</td>
<td>Y</td>
<td>2014-09-12 13:24:06</td>
<td>1602</td>
</tr>
</tbody>
</table>

Free space for compressed user config files: 1519616
```
show arp:
ARP Cache Timeout: 1200 (seconds)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.2</td>
<td>70-72-CF-83-34-66</td>
<td>other</td>
<td>VLAN1</td>
</tr>
<tr>
<td>192.168.0.99</td>
<td>00-60-6E-00-5F-A1</td>
<td>dynamic</td>
<td>VLAN1</td>
</tr>
</tbody>
</table>

Total entry : 2

show interfaces brief:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Status</th>
<th>PVID</th>
<th>Pri</th>
<th>Speed/Duplex</th>
<th>Type</th>
<th>Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>Up</td>
<td>1</td>
<td>0</td>
<td>Auto-100full</td>
<td>1000BASE-T</td>
<td>None</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>Down</td>
<td>1</td>
<td>0</td>
<td>Auto</td>
<td>1000BASE-T</td>
<td>None</td>
</tr>
<tr>
<td>Eth 1/3</td>
<td>Down</td>
<td>1</td>
<td>0</td>
<td>Auto</td>
<td>1000BASE-T</td>
<td>None</td>
</tr>
<tr>
<td>Eth 1/4</td>
<td>Down</td>
<td>1</td>
<td>0</td>
<td>Auto</td>
<td>1000BASE-T</td>
<td>None</td>
</tr>
<tr>
<td>Eth 1/5</td>
<td>Down</td>
<td>1</td>
<td>0</td>
<td>Auto</td>
<td>1000BASE-T</td>
<td>None</td>
</tr>
</tbody>
</table>

:

show adoption status:
Not adopted to any wireless controller

show adoption history:
No history

Console#

**show users**  Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

**Default Setting**
None

**Command Mode**
Normal Exec, Privileged Exec

**Command Usage**
The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

**Example**

```
Console#show users
User Name Accounts:
User Name | Privilege | Public-Key
-----------|-----------|-----------
admin      | 15        | None      
guest      | 0         | None      
steve      | 15        | RSA       

Online Users:
Line | Session ID | User Name | Idle Time (h:m:s) | Remote IP Addr
----|------------|----------|-------------------|-----------------|
*Console | 0 | admin | 0:00:00 |  
Telnet | 1 | admin | 0:00:00 | 192.168.1.19  
Telnet | 2 | SSH 1 | 0:00:06 | 192.168.1.19  
```
Chapter 4 | System Management Commands

System Status

Web Online Users:

<table>
<thead>
<tr>
<th>Line</th>
<th>User Name</th>
<th>Idle time (h:m:s)</th>
<th>Remote IP addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>admin</td>
<td>0:00:05</td>
<td>192.168.0.99</td>
</tr>
</tbody>
</table>

Console#

**show version**  This command displays hardware and software version information for the system.

**Command Mode**

Normal Exec, Privileged Exec

**Example**

```
Console#show version
Unit 1
Serial Number          : 14053520900018
Hardware Version       : R01
EPLD Version           : 0.00
Number of Ports        : 28
Main Power Status      : Up
Role                   : Master
Loader Version         : 5.0.0.1-01A
Linux Kernel Version   : 2.6.22.18
Boot ROM Version       : 0.0.0.1
Operation Code Version : 5.0.0.0-03D
Adoptd Version         : 5.8.0.0-208812X

Console#
```

**Table 12: show version – display description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>The serial number of the switch.</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Hardware version of the main board.</td>
</tr>
<tr>
<td>EPLD Version</td>
<td>Version number of Erasable Programmable Logic Device.</td>
</tr>
<tr>
<td>Number of Ports</td>
<td>Number of built-in ports.</td>
</tr>
<tr>
<td>Main Power Status</td>
<td>Displays the status of the internal power supply.</td>
</tr>
<tr>
<td>Role</td>
<td>Shows that this switch is operating as Master or Slave.</td>
</tr>
<tr>
<td>Loader Version</td>
<td>Version number of loader code.</td>
</tr>
<tr>
<td>Linux Kernel Version</td>
<td>Version number of Linux kernel.</td>
</tr>
<tr>
<td>Boot ROM Version</td>
<td>Version of Power-On Self-Test (POST) and boot code.</td>
</tr>
<tr>
<td>Operation Code Version</td>
<td>Version number of runtime code.</td>
</tr>
<tr>
<td>Adoptd Version</td>
<td>Version number of adopted device code.</td>
</tr>
</tbody>
</table>
**show watchdog**  This command shows if watchdog debugging is enabled.

**Command Mode**
Privileged Exec

**Example**

```console
Console#show watchdog
Software Watchdog Information
 Status :  Enabled
Console#
```

**watchdog software**  This command monitors key processes, and automatically reboots the system if any of these processes are not responding correctly.

**Syntax**

`watchdog software {disable | enable}`

**Default Setting**
Disabled

**Command Mode**
Privileged Exec

**Example**

```console
Console#watchdog software enable
Console#
```

---

### Frame Size

This section describes commands used to configure the Ethernet frame size on the switch.

**Table 13: Frame Size Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>jumbo frame</td>
<td>Enables support for jumbo frames</td>
<td>GC</td>
</tr>
</tbody>
</table>

**jumbo frame**  This command enables support for Layer 2 jumbo frames for Gigabit Ethernet ports. Use the `no` form to disable it.

**Syntax**

`[no] jumbo frame`
Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
◆ This switch provides more efficient throughput for large sequential data transfers by supporting Layer 2 jumbo frames on Gigabit Ethernet ports or trunks up to 10240 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

◆ To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

◆ The current setting for jumbo frames can be displayed with the show system command.

Example

```
Console(config)#jumbo frame
Console(config)#
```

File Management

Managing Firmware

Firmware can be uploaded and downloaded to or from an FTP/TFTP server. By saving runtime code to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from an FTP/TFTP server. The configuration file can be later downloaded to restore switch settings.
The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the FTP/TFTP server, but cannot be used as the destination on the switch.

Table 14: Flash/File Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the file or image used to start up the system</td>
<td>GC</td>
</tr>
<tr>
<td>copy</td>
<td>Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server</td>
<td>PE</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file or code image</td>
<td>PE</td>
</tr>
<tr>
<td>dir</td>
<td>Displays a list of files in flash memory</td>
<td>PE</td>
</tr>
<tr>
<td>whichboot</td>
<td>Displays the files booted</td>
<td>PE</td>
</tr>
<tr>
<td><strong>Automatic Code Upgrade Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>upgrade opcode auto</td>
<td>Automatically upgrades the current image when a new version is detected on the indicated server</td>
<td>GC</td>
</tr>
<tr>
<td>upgrade opcode path</td>
<td>Specifies an FTP/TFTP server and directory in which the new opcode is stored</td>
<td>GC</td>
</tr>
<tr>
<td>upgrade opcode reload</td>
<td>Reloads the switch automatically after the opcode upgrade is completed</td>
<td>GC</td>
</tr>
<tr>
<td>show upgrade</td>
<td>Shows the opcode upgrade configuration settings.</td>
<td>PE</td>
</tr>
<tr>
<td><strong>TFTP Configuration Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip tftp retry</td>
<td>Specifies the number of times the switch can retry transmitting a request to a TFTP server</td>
<td>GC</td>
</tr>
<tr>
<td>ip tftp timeout</td>
<td>Specifies the time the switch can wait for a response from a TFTP server before retransmitting a request or timing out for the last retry</td>
<td>GC</td>
</tr>
<tr>
<td>show ip tftp</td>
<td>Displays information about TFTP settings</td>
<td>PE</td>
</tr>
</tbody>
</table>

**General Commands**

**boot system**  This command specifies the file or image used to start up the system.

**Syntax**

```
boot system (boot-rom | config | opcode): filename
```

- **boot-rom** - Boot ROM.
- **config** - Configuration file.
- **opcode** - Run-time operation code.
- **filename** - Name of configuration file or code image.

* The colon (:) is required.
Default Setting
None

Command Mode
Global Configuration

Command Usage
◆ A colon (:) is required after the specified file type.
◆ If the file contains an error, it cannot be set as the default file.

Example
```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands
dir (114)
whichboot (115)

copy
This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Syntax
```
copy file {file | ftp | running-config | startup-config | tftp}
copy ftp {add-to-running-config | file | https-certificate | public-key | running-config | startup-config}
copy running-config {file | ftp | startup-config | tftp}
copy startup-config {file | ftp | running-config | tftp}
copy tftp {add-to-running-config | file | https-certificate | public-key | running-config | startup-config}
```

- **add-to-running-config** - Keyword that adds the settings listed in the specified file to the running configuration.
- **file** - Keyword that allows you to copy to/from a file.
- **ftp** - Keyword that allows you to copy to/from an FTP server.
- **https-certificate** - Keyword that allows you to copy the HTTPS secure site certificate.
- **public-key** - Keyword that allows you to copy a SSH key from a TFTP server.

(See “Secure Shell” on page 234.)
**running-config** - Keyword that allows you to copy to/from the current running configuration.

**startup-config** - The configuration used for system initialization.

**tftp** - Keyword that allows you to copy to/from a TFTP server.

---

**Default Setting**

None

---

**Command Mode**

Privileged Exec

---

**Command Usage**

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 127 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, “,” ,” “)
- The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.
- You can use “Factory_Default_Config.cfg” as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- For information on specifying an https-certificate, see “Replacing the Default Secure-site Certificate” in the System Reference Guide. For information on configuring the switch to use HTTPS for a secure connection, see the ip http secure-server command.
- When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that “anonymous” is set as the default user name.

---

**Example**

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
  1. config; 2. opcode; 3. loader: 2
Source file name: m360.bix
Destination file name: m360.bix

Write to FLASH Programming.
```
The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
  1. config;  2. opcode;  1
Source file name: startup
TFTP server IP address: 10.1.0.99
Destination file name: startup.01
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
Destination configuration file name: startup
Flash programming started.
Flash programming completed.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Flash programming started.
Flash programming completed.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********
Success.
Console#reload
System will be restarted, continue <y/n>? y
```
This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
  1. RSA:  2. DSA: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

This example shows how to copy a file to an FTP server.

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[*****]: ****
Choose file type:
  1. config:  2. opcode: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX

Console#
```

delete  This command deletes a file or image.

**Syntax**

```
delete file name  filename
```

*filename* - Name of configuration file or code image.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Command Usage**

◆ If the file type is used for system startup, then this file cannot be deleted.

◆ “Factory_Default_Config.cfg” cannot be deleted.
Example
This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete file name test2.cfg
Console#
```

Related Commands
dir (114)
delete public-key (240)

dir
This command displays a list of files in flash memory.

Syntax
```
dir {boot-rom: | config: | opcode:} [filename]
```

- `boot-rom` - Boot ROM (or diagnostic) image file.
- `config` - Switch configuration file.
- `opcode` - Run-time operation code image file.

`filename` - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting
None

Command Mode
Privileged Exec

Command Usage
If you enter the command `dir` without any parameters, the system displays all files.

File information is shown below:

Table 15: File Directory Information

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>The name of the file.</td>
</tr>
<tr>
<td>File Type</td>
<td>File types: Boot-Rom, Operation Code, and Config file.</td>
</tr>
<tr>
<td>Startup</td>
<td>Shows if this file is used when the system is started.</td>
</tr>
<tr>
<td>Create Time</td>
<td>The date and time the file was created.</td>
</tr>
<tr>
<td>Size</td>
<td>The length of the file in bytes.</td>
</tr>
</tbody>
</table>
**Example**
The following example shows how to display all file information:

```console
Console#dir
File Name                  Type   Startup Modify Time         Size(bytes)
-------------------------- -------------- ------- ------------------- ----------
EX3548_Op_V4.0.1.0-01I.bix       OpCode     N    1970-01-01 00:00:00    7634132
Factory_Default_Config.cfg       Config     N    2014-08-24 06:40:02        455
startup1.cfg                     Config     Y    2014-09-12 13:24:06       1602
-----------------------------------------------------------------------------
Free space for compressed user config files:   1355776
Console#
```

**whichboot**  
This command displays which files were booted when the system powered up.

**Syntax**

```
whichboot
```

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

This example shows the information displayed by the `whichboot` command. See the table under the `dir` command for a description of the file information displayed by this command.

```console
Console#whichboot
File Name                  Type  Startup Modify Time         Size(bytes)
-------------------------------- ------- ------- ------------------- ----------
Unit 1:
startup1.cfg                     Config     Y    2014-09-12 13:24:06       1602
Console#
```

**Automatic Code Upgrade Commands**

**upgrade opcode auto**  
This command automatically upgrades the current operational code when a new version is detected on the server indicated by the `upgrade opcode path` command. Use the `no` form of this command to restore the default setting.

**Syntax**

```
[no] upgrade opcode auto
```
Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
◆ This command is used to enable or disable automatic upgrade of the operational code. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:

1. It will search for a new version of the image at the location specified by upgrade opcode path command. The name for the new image stored on the TFTP server must be EX3500_Op.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.

2. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.

3. It sets the new version as the startup image.

4. It then restarts the system to start using the new image.

◆ Any changes made to the default setting can be displayed with the show running-config or show startup-config commands.

Example

```console
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

If a new image is found at the specified location, the following type of messages will be displayed during bootup:

```
::
Automatic Upgrade is looking for a new image
New image detected: current version 1.0.1.5; new version 1.1.2.0
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
::
```
**upgrade opcode path**  
This command specifies an TFTP server and directory in which the new opcode is stored. Use the *no* form of this command to clear the current setting.

**Syntax**

```
upgrade opcode path opcode-dir-url
no upgrade opcode path
```

- The location of the new code.

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- This command is used in conjunction with the *upgrade opcode auto* command to facilitate automatic upgrade of new operational code stored at the location indicated by this command.

- The name for the new image stored on the TFTP server must be EX3500_Op.bix. However, note that file name is not to be included in this command.

- When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  ```
tftp://192.168.0.1[/filedir]/
  ```

- When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  ```
ftp://[username[:password@]]192.168.0.1[/filedir]/
  ```

If the user name is omitted, “anonymous” will be used for the connection. If the password is omitted a null string (“”) will be used for the connection.

**Example**

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://zebra:billy@192.168.0.1/sm24/
Console(config)#
```
**upgrade opcode reload**  This command reloads the switch automatically after the opcode upgrade is completed. Use the no form to disable this feature.

**Syntax**

```
[no] upgrade opcode reload
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Example**

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode reload
Console(config)#
```

**show upgrade**  This command shows the opcode upgrade configuration settings.

**Command Mode**

Privileged Exec

**Example**

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status    : Disabled
  Reload Status : Disabled
  Path      :
  File Name : EX3500_Op.bix
Console#
```

**TFTP Configuration Commands**

**ip tftp retry**  This command specifies the number of times the switch can retry transmitting a request to a TFTP server after waiting for the configured timeout period and receiving no response. Use the no form to restore the default setting.

**Syntax**

```
  ip tftp retry retries
  no ip tftp retry
```

*retries* - The number of times the switch can resend a request to a TFTP server before it aborts the connection. (Range: 1-16)
**Default Setting**
15

**Command Mode**
Global Configuration

**Example**

```
Console(config)#ip tftp retry 10
Console(config)#
```

**ip tftp timeout**
This command specifies the time the switch can wait for a response from a TFTP server before retransmitting a request or timing out for the last retry. Use the no form to restore the default setting.

**Syntax**

```
ip tftp timeout seconds
no ip tftp timeout
```

- The time the switch can wait for a response from a TFTP server before retransmitting a request or timing out. (Range: 1-65535 seconds)

**Default Setting**
5 seconds

**Command Mode**
Global Configuration

**Example**

```
Console(config)#ip tftp timeout 10
Console(config)#
```

**show ip tftp**
This command displays information about the TFTP settings configured on this switch.

**Syntax**

```
show ip tftp
```

**Command Mode**
Privileged Exec
You can access the onboard configuration program by attaching a VT100 compatible device to the server’s serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

### Table 16: Line Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>Identifies a specific line for configuration and starts the line configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>accounting exec</td>
<td>Applies an accounting method to local console, Telnet or SSH connections</td>
<td>LC</td>
</tr>
<tr>
<td>authorization exec</td>
<td>Applies an authorization method to local console, Telnet or SSH connections</td>
<td>LC</td>
</tr>
<tr>
<td>databits*</td>
<td>Sets the number of data bits per character that are interpreted and generated by hardware</td>
<td>LC</td>
</tr>
<tr>
<td>exec-timeout</td>
<td>Sets the interval that the command interpreter waits until user input is detected</td>
<td>LC</td>
</tr>
<tr>
<td>login</td>
<td>Enables password checking at login</td>
<td>LC</td>
</tr>
<tr>
<td>parity*</td>
<td>Defines the generation of a parity bit</td>
<td>LC</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password on a line</td>
<td>LC</td>
</tr>
<tr>
<td>password-thresh</td>
<td>Sets the password intrusion threshold, which limits the number of failed logon attempts</td>
<td>LC</td>
</tr>
<tr>
<td>silent-time*</td>
<td>Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command</td>
<td>LC</td>
</tr>
<tr>
<td>speed*</td>
<td>Sets the terminal baud rate</td>
<td>LC</td>
</tr>
<tr>
<td>stopbits*</td>
<td>Sets the number of the stop bits transmitted per byte</td>
<td>LC</td>
</tr>
<tr>
<td>timeout login response</td>
<td>Sets the interval that the system waits for a login attempt</td>
<td>LC</td>
</tr>
<tr>
<td>disconnect</td>
<td>Terminates a line connection</td>
<td>PE</td>
</tr>
<tr>
<td>show line</td>
<td>Displays a terminal line's parameters</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

* These commands only apply to the serial port.
**line**  This command identifies a specific line for configuration, and to process subsequent line configuration commands.

**Syntax**

```
line {console | vty}
```

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

**Default Setting**

There is no default line.

**Command Mode**

Global Configuration

**Command Usage**

Telnet is considered a virtual terminal connection and will be shown as “VTY” in screen displays such as `show users`. However, the serial communication parameters (e.g., `databits`) do not affect Telnet connections.

**Example**

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line-console)#
```

**Related Commands**

- `show line (130)`
- `show users (105)`

**databits**  This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

**Syntax**

```
databits {7 | 8}
```

**no databits**

- **7** - Seven data bits per character.
- **8** - Eight data bits per character.

**Default Setting**

8 data bits per character

**Command Mode**

Line Configuration
**Command Usage**

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

**Example**

To specify 7 data bits, enter this command:

```
Console(config-line-console)#databits 7
Console(config-line-console)#
```

**Related Commands**

`parity (124)`

**exec-timeout**

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

**Syntax**

```
exec-timeout [seconds]
no exec-timeout
```

- `seconds` - Integer that specifies the timeout interval.
  (Range: 60 - 65535 seconds; 0: no timeout)

**Default Setting**

600 seconds (10 minutes)

**Command Mode**

Line Configuration

**Command Usage**

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.

- This command applies to both the local console and Telnet connections.

- The timeout for Telnet cannot be disabled.

- Using the command without specifying a timeout restores the default setting.

**Example**

To set the timeout to two minutes, enter this command:

```
Console(config-line-console)#exec-timeout 120
Console(config-line-console)#
```
**login**  This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

**Syntax**

```
login [local]
no login
```

- **local** - Selects local password checking. Authentication is based on the user name specified with the **username** command.

**Default Setting**

login local

**Command Mode**

Line Configuration

**Command Usage**

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user’s privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

**Example**

```
Console(config-line-console)#login local
Console(config-line-console)#
```

**Related Commands**

- **username** (205)
- **password** (124)
**parity**  This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

**Syntax**

\[
\text{parity \{none | even | odd\}}
\]

\[
\text{no parity}
\]

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

**Default Setting**
No parity

**Command Mode**
Line Configuration

**Command Usage**
Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

**Example**
To specify no parity, enter this command:

```
Console(config-line-console)#parity none
Console(config-line-console)#
```

**password**  This command specifies the password for a line. Use the **no** form to remove the password.

**Syntax**

\[
\text{password \{0 | 7\} password}
\]

\[
\text{no password}
\]

- **0 | 7** - 0 means plain password, 7 means encrypted password
- **password** - Character string that specifies the line password.
  (Maximum length: 32 characters plain text or encrypted, case sensitive)

**Default Setting**
No password is specified.

**Command Mode**
Line Configuration
Command Usage

◆ When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the password-thresh command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.

◆ The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line-console)#password 0 secret
Console(config-line-console)#
```

Related Commands

login (123)
password-thresh (125)

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

```
password-thresh [threshold]
no password-thresh
```

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent-time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
Example
To set the password threshold to five attempts, enter this command:

```
Console(config-line-console)#password-thresh 5
Console(config-line-console)#
```

Related Commands
silent-time (126)

silent-time This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command. Use the no form to remove the silent time value.

Syntax
```
silent-time [seconds]
no silent-time
```

seconds - The number of seconds to disable console response. (Range: 0-65535; where 0 means disabled)

Default Setting
Disabled

Command Mode
Line Configuration

Example
To set the silent time to 60 seconds, enter this command:

```
Console(config-line-console)#silent-time 60
Console(config-line-console)#
```

Related Commands
password-thresh (125)
**speed**  This command sets the terminal line’s baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

**Syntax**

```
speed bps
no speed
```

*bps* - Baud rate in bits per second.

(Options: 9600, 19200, 38400, 57600, 115200 bps)

**Default Setting**

115200 bps

**Command Mode**

Line Configuration

**Command Usage**

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

**Note:**  Auto-detection of baud rate is only performed at user log in.

**Note:**  Due to a hardware limitation, the terminal program connected to the console port must be set to 8 data bits when using auto baud rate detection.

---

**Example**

To specify 57600 bps, enter this command:

```
Console(config-line-console)#speed 57600
Console(config-line-console)#
```

**stopbits**  This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

**Syntax**

```
stopbits {1 | 2}
no stopbits
```

*1* - One stop bit

*2* - Two stop bits
Default Setting
1 stop bit

Command Mode
Line Configuration

Example
To specify 2 stop bits, enter this command:

```
Console(config-line-console)#stopbits 2
Console(config-line-console)#
```

**timeout login response**
This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

**Syntax**
```
timeout login response [seconds]
no timeout login response
```

- **seconds** - Integer that specifies the timeout interval.
- (Range: 10 - 300 seconds)

Default Setting
300 seconds

Command Mode
Line Configuration

**Command Usage**
- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

**Example**
To set the timeout to two minutes, enter this command:

```
Console(config-line-console)#timeout login response 120
Console(config-line-console)#
```
**disconnect**  This command terminates an SSH, Telnet, or console connection.

**Syntax**

```
disconnect session-id
```

*session-id* — The session identifier for an SSH, Telnet or console connection.  
(Range: 0-8)

**Command Mode**

Privileged Exec

**Command Usage**

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

**Example**

```
Console#disconnect 1
Console#
```

**Related Commands**

- show ssh (244)
- show users (105)

**terminal**  This command configures terminal settings, including escape-character, lines displayed, terminal type, width, and command history. Use the no form with the appropriate keyword to restore the default setting.

**Syntax**

```
terminal {escape-character {ASCII-number | character} | history [size size] | length length | terminal-type {ansi-bbs | vt-100 | vt-102} | width width}
```

*escape-character* - The keyboard character used to escape from current line input.

*ASCII-number* - ASCII decimal equivalent. (Range: 0-255)

*character* - Any valid keyboard character.

*history* - The number of lines stored in the command buffer, and recalled using the arrow keys. (Range: 0-256)

*length* - The number of lines displayed on the screen. (Range: 24-200, where 0 means not to pause)

*terminal-type* - The type of terminal emulation used.

*ansi-bbs* - ANSI-BBS

*vt-100* - VT-100

*vt-102* - VT-102
width - The number of character columns displayed on the terminal.
(Range: 0-80)

Default Setting
Escape Character: 27 (ASCII-number)
History: 10
Length: 24
Terminal Type: VT100
Width: 80

Command Mode
Privileged Exec

Example
This example sets the number of lines displayed by commands with lengthy output such as `show running-config` to 48 lines.

```
Console#terminal length 48
Console#
```

show line   This command displays the terminal line's parameters.

Syntax

```
show line [console | vty]
```

*console* - Console terminal line.
*vty* - Virtual terminal for remote console access (i.e., Telnet).

Default Setting
Shows all lines

Command Mode
Normal Exec, Privileged Exec

Example
To show all lines, enter this command:

```
Console#show line
Terminal Configuration for this session:
Length              : 24
Width               : 80
History Size        : 10
Escape Character(ASCII-number) : 27
Terminal Type       : VT100

Console Configuration:
Password Threshold : 3 times
EXEC Timeout       : 600 seconds
Login Timeout      : 300 seconds
```
Event Logging

This section describes commands used to configure event logging on the switch.

Table 17: Event Logging Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging facility</td>
<td>Sets the facility type for remote logging of syslog messages</td>
<td>GC</td>
</tr>
<tr>
<td>logging history</td>
<td>Limits syslog messages saved to switch memory based on severity</td>
<td>GC</td>
</tr>
<tr>
<td>logging host</td>
<td>Adds a syslog server host IP address that will receive logging messages</td>
<td>GC</td>
</tr>
<tr>
<td>logging on</td>
<td>Controls logging of error messages</td>
<td>GC</td>
</tr>
<tr>
<td>logging trap</td>
<td>Limits syslog messages saved to a remote server based on severity</td>
<td>GC</td>
</tr>
<tr>
<td>clear log</td>
<td>Clears messages from the logging buffer</td>
<td>PE</td>
</tr>
<tr>
<td>show log</td>
<td>Displays log messages</td>
<td>PE</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of logging</td>
<td>PE</td>
</tr>
</tbody>
</table>

logging facility

This command sets the facility type for remote logging of syslog messages. Use the no form to return the type to the default.

Syntax

```
logging facility type
no logging facility
```

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23
Command Mode
Global Configuration

Command Usage
The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example
```
Console(config)#logging facility 19
```

**logging history**
This command limits syslog messages saved to switch memory based on severity. The no form returns the logging of syslog messages to the default level.

Syntax
```
logging history {flash | ram} level
no logging history {flash | ram}
```

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- **level** - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

**Table 18: Logging Levels**

<table>
<thead>
<tr>
<th>Level</th>
<th>Severity Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>debugging</td>
<td>Debugging messages</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
<td>Informational messages only</td>
</tr>
<tr>
<td>5</td>
<td>notifications</td>
<td>Normal but significant condition, such as cold start</td>
</tr>
<tr>
<td>4</td>
<td>warnings</td>
<td>Warning conditions (e.g., return false, unexpected return)</td>
</tr>
<tr>
<td>3</td>
<td>errors</td>
<td>Error conditions (e.g., invalid input, default used)</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
<td>Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)</td>
</tr>
<tr>
<td>1</td>
<td>alerts</td>
<td>Immediate action needed</td>
</tr>
<tr>
<td>0</td>
<td>emergencies</td>
<td>System unusable</td>
</tr>
</tbody>
</table>

**Default Setting**
- Flash: errors (level 3 - 0)
- RAM: debugging (level 7 - 0)
Command Mode
Global Configuration

Command Usage
The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host
This command adds a syslog server host IP address that will receive logging messages. Use the no form to remove a syslog server host.

Syntax

```
logging host host-ip-address [port udp-port]
no logging host host-ip-address
```

- host-ip-address - The IPv4 or IPv6 address of a syslog server.
- udp-port - UDP port number used by the remote server. (Range: 1-65535)

Default Setting
None

Command Mode
Global Configuration

Command Usage
◆ Use this command more than once to build up a list of host IP addresses.
◆ The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging on
This command controls logging of error messages, sending debug or error messages to a logging process. The no form disables the logging process.

Syntax

```
[no] logging on
```
Default Setting
None

Command Mode
Global Configuration

Command Usage
The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the logging history command to control the type of error messages that are stored in memory. You can use the logging trap command to control the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
```

Related Commands
logging history (132)
logging trap (134)
clear log (135)

logging trap
This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the no form to disable remote logging.

Syntax

```
logging trap [level level]
no logging trap [level]
```

- `level` - One of the syslog severity levels listed in the table on page 132. Messages sent include the selected level through level 0.

Default Setting
Disabled
Level 7

Command Mode
Global Configuration

Command Usage
- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

**Example**

```
Console(config)#logging trap 4
Console(config)#
```

**clear log** This command clears messages from the log buffer.

**Syntax**

```
clear log [flash | ram]
```

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

**Default Setting**

Flash and RAM

**Command Mode**

Privileged Exec

**Example**

```
Console#clear log
Console#
```

**Related Commands**

- `show log (135)`

**show log** This command displays the log messages stored in local memory.

**Syntax**

```
show log {flash | ram}
```

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

**Default Setting**

None

**Command Mode**

Privileged Exec
**Command Usage**

- All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).

- All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

**Example**
The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
  "VLAN 1 link-up notification."
  level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
  "Unit 1, Port 1 link-up notification."
  level: 6, module: 5, function: 1, and event no.: 1
Console#
```

**show logging**
This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

**Syntax**

```
show logging {flash | ram | sendmail | trap}
```

- `flash` - Displays settings for storing event messages in flash memory (i.e., permanent memory).
- `ram` - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).
- `sendmail` - Displays settings for the SMTP event handler (page 141).
- `trap` - Displays settings for the trap function.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**
The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), and the message level for RAM is “debugging” (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:   Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:   Enabled
```
History logging in RAM: level debugging
Console#

The following example displays settings for the trap function. Console# show logging

Table 19: show logging flash/ram - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog logging</td>
<td>Shows if system logging has been enabled via the <code>logging on</code> command.</td>
</tr>
<tr>
<td>History logging in FLASH</td>
<td>The message level(s) reported based on the <code>logging history</code> command.</td>
</tr>
<tr>
<td>History logging in RAM</td>
<td>The message level(s) reported based on the <code>logging history</code> command.</td>
</tr>
</tbody>
</table>

```
Remote Log Status : Enabled
Remote Log Facility Type : Local use 7
Remote Log Level Type : Debugging messages
Remote Log Server IP Address : 1.2.3.4
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0

Console#
```

Table 20: show logging trap - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Log Status</td>
<td>Shows if remote logging has been enabled via the <code>logging trap</code> command.</td>
</tr>
<tr>
<td>Remote Log Facility Type</td>
<td>The facility type for remote logging of syslog messages as specified in the <code>logging facility</code> command.</td>
</tr>
<tr>
<td>Remote Log Level Type</td>
<td>The severity threshold for syslog messages sent to a remote server as specified in the <code>logging trap</code> command.</td>
</tr>
<tr>
<td>Remote Log Server IP Address</td>
<td>The address of syslog servers as specified in the <code>logging host</code> command.</td>
</tr>
</tbody>
</table>

Related Commands
show logging sendmail (141)
SMTP Alerts

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 21: Event Logging Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging sendmail</td>
<td>Enables SMTP event handling</td>
<td>GC</td>
</tr>
<tr>
<td>logging sendmail host</td>
<td>SMTP servers to receive alert messages</td>
<td>GC</td>
</tr>
<tr>
<td>logging sendmail level</td>
<td>Severity threshold used to trigger alert messages</td>
<td>GC</td>
</tr>
<tr>
<td>logging sendmail</td>
<td>Email recipients of alert messages</td>
<td>GC</td>
</tr>
<tr>
<td>destination-email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>logging sendmail</td>
<td>Email address used for “From” field of alert messages</td>
<td>GC</td>
</tr>
<tr>
<td>source-email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show logging sendmail</td>
<td>Displays SMTP event handler settings</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

logging sendmail

This command enables SMTP event handling. Use the no form to disable this function.

Syntax

[no] logging sendmail

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the no form to remove an SMTP server.

Syntax

[no] logging sendmail host ip-address

ip-address - IPv4 address of an SMTP server that will be sent alert messages for event handling.
SMTP Alerts

Default Setting
None

Command Mode
Global Configuration

Command Usage
◆ You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
◆ To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
◆ To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level
This command sets the severity threshold used to trigger alert messages. Use the no form to restore the default setting.

Syntax

```
logging sendmail level level
no logging sendmail level
```

- One of the system message levels (page 132). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting
Level 7

Command Mode
Global Configuration

Command Usage
The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)
Example
This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail destination-email
This command specifies the email recipients of alert messages. Use the `no` form to remove a recipient.

Syntax
```
[no] logging sendmail destination-email email-address
```

- `email-address` - The source email address used in alert messages.
  (Range: 1-41 characters)

Default Setting
None

Command Mode
Global Configuration

Command Usage
You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example
```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail source-email
This command sets the email address used for the “From” field in alert messages. Use the `no` form to restore the default value.

Syntax
```
logging sendmail source-email email-address

no logging sendmail source-email
```

- `email-address` - The source email address used in alert messages.
  (Range: 1-41 characters)

Default Setting
None

Command Mode
Global Configuration
Command Usage
You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

show logging sendmail This command displays the settings for the SMTP event handler.

Command Mode
Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
192.168.1.19

SMTP Minimum Severity Level: 7
SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP Source Email Address: bill@this-company.com
SMTP Status: Enabled
Console#
```

Time

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 22: Time Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNTP Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sntp client</td>
<td>Accepts time from specified time servers</td>
<td>GC</td>
</tr>
<tr>
<td>sntp poll</td>
<td>Sets the interval at which the client polls for time</td>
<td>GC</td>
</tr>
<tr>
<td>sntp server</td>
<td>Specifies one or more time servers</td>
<td>GC</td>
</tr>
<tr>
<td>show sntp</td>
<td>Shows current SNTP configuration settings</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>
SNTP Commands

**snntp client**  This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the `snntp server` command. Use the **no** form to disable SNTP client requests.

### Syntax

```
[no] snntp client
```

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (e.g., Dec 1 10:01:35 2014).

- This command enables client time requests to time servers specified via the `snntp server` command. It issues time synchronization requests based on the interval set via the `snntp poll` command.

---

**Table 22: Time Commands (Continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NTP Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntp authenticate</td>
<td>Enables authentication for NTP traffic</td>
<td>GC</td>
</tr>
<tr>
<td>ntp authentication-key</td>
<td>Configures authentication keys</td>
<td>GC</td>
</tr>
<tr>
<td>ntp client</td>
<td>Enables the NTP client for time updates from specified servers</td>
<td>GC</td>
</tr>
<tr>
<td>ntp server</td>
<td>Specifies NTP servers to poll for time updates</td>
<td>GC</td>
</tr>
<tr>
<td>show ntp</td>
<td>Shows current NTP configuration settings</td>
<td>NE, PE</td>
</tr>
<tr>
<td><strong>Manual Configuration Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>clock summer-time (date)</td>
<td>Configures summer time* for the switch's internal clock</td>
<td>GC</td>
</tr>
<tr>
<td>clock summer-time (predefined)</td>
<td>Configures summer time* for the switch's internal clock</td>
<td>GC</td>
</tr>
<tr>
<td>clock summer-time (recurring)</td>
<td>Configures summer time* for the switch's internal clock</td>
<td>GC</td>
</tr>
<tr>
<td>clock timezone</td>
<td>Sets the time zone for the switch's internal clock</td>
<td>GC</td>
</tr>
<tr>
<td>calendar set</td>
<td>Sets the system date and time</td>
<td>PE</td>
</tr>
<tr>
<td>show calendar</td>
<td>Displays the current date and time setting</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

* Daylight savings time.
Example

```console
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current Time:  Dec 23 02:52:44 2002
Poll Interval: 60
Current Mode: unicast
SNTP Status : Enabled
SNTP Server 137.92.140.80 0.0.0.0 0.0.0.0
Current Server: 137.92.140.80
Console#
```

Related Commands

- `sntp server (144)`
- `sntp poll (143)`
- `show sntp (144)`

**sntp poll**  This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the `no` form to restore to the default.

**Syntax**

```plaintext
sntp poll seconds
no sntp poll
```

- `seconds` - Interval between time requests. (Range: 16-16384 seconds)

**Default Setting**

16 seconds

**Command Mode**

Global Configuration

**Example**

```console
Console(config)#sntp poll 60
Console#
```

Related Commands

- `sntp client (142)`
**sntp server**  
This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the no form to clear all time servers from the current list, or to clear a specific server.

**Syntax**
```
sntp server [ip1 [ip2 [ip3]]]
no sntp server [ip1 [ip2 [ip3]]]
```

*ip* - IP address of a time server (NTP or SNTP). (Range: 1 - 3 addresses)

**Default Setting**
None

**Command Mode**
Global Configuration

**Command Usage**
This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

**Example**
```
Console(config)#sntp server 10.1.0.19
Console#
```

**Related Commands**
- sntp client (142)
- sntp poll (143)
- show sntp (144)

**show sntp**  
This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

**Command Mode**
Normal Exec, Privileged Exec

**Command Usage**
This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).
Example

```
Console#show sntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80 0.0.0.0 0.0.0.0
Current Server : 137.92.140.80
Console#
```

NTP Commands

**ntp authenticate**  This command enables authentication for NTP client-server communications. Use the **no** form to disable authentication.

**Syntax**

```
[no] ntp authenticate
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

**Example**

```
Console(config)#ntp authenticate
Console(config)#
```

**Related Commands**

*ntp authentication-key (146)*
ntp authentication-key  This command configures authentication keys and key numbers to use when NTP authentication is enabled. Use the no form of the command to clear a specific authentication key or all keys from the current list.

Syntax

```
ntp authentication-key number md5 key
no ntp authentication-key [number]
```

- `number` - The NTP authentication key ID number. (Range: 1-65535)
- `md5` - Specifies that authentication is provided by using the message digest algorithm 5.
- `key` - An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

Default Setting
None

Command Mode
Global Configuration

Command Usage

- The key number specifies a key value in the NTP authentication key list. Up to 255 keys can be configured on the switch. Re-enter this command for each server you want to configure.

- Note that NTP authentication key numbers and values must match on both the server and client.

- NTP authentication is optional. When enabled with the `ntp authenticate` command, you must also configure at least one key number using this command.

- Use the no form of this command without an argument to clear all authentication keys in the list.

Example

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

Related Commands
ntp authenticate (145)
**ntp client**  This command enables NTP client requests for time synchronization from NTP time servers specified with the `ntp servers` command. Use the `no` form to disable NTP client requests.

**Syntax**

```
[no] ntp client
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- The SNTP and NTP clients cannot be enabled at the same time. First disable the SNTP client before using this command.

- The time acquired from time servers is used to record accurate dates and times for log events. Without NTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).

- This command enables client time requests to time servers specified via the `ntp servers` command. It issues time synchronization requests based on the interval set via the `ntp poll` command.

**Example**

```
Console(config)#ntp client
Console(config)#
```

**Related Commands**

- `sntp client (142)`
- `ntp server (147)`

**ntp server**  This command sets the IP addresses of the servers to which NTP time requests are issued. Use the `no` form of the command to clear a specific time server or all servers from the current list.

**Syntax**

```
ntp server ip-address [key key-number]
no ntp server [ip-address]
```

- `ip-address` - IP address of an NTP time server.
- `key-number` - The number of an authentication key to use in communications with the server. (Range: 1-65535)
Default Setting
Version number: 3

Command Mode
Global Configuration

Command Usage
◆ This command specifies time servers that the switch will poll for time updates when set to NTP client mode. It issues time synchronization requests based on the interval set with the ntp poll command. The client will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.

◆ You can configure up to 50 NTP servers on the switch. Re-enter this command for each server you want to configure.

◆ NTP authentication is optional. If enabled with the ntp authenticate command, you must also configure at least one key number using the ntp authentication-key command.

◆ Use the no form of this command without an argument to clear all configured servers in the list.

Example

```
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#
```

Related Commands
ntp client (147)
show ntp (148)

show ntp
This command displays the current time and configuration settings for the NTP client, and indicates whether or not the local time has been properly updated.

Command Mode
Normal Exec, Privileged Exec

Command Usage
This command displays the current time, the poll interval used for sending time synchronization requests, and the current NTP mode (i.e., unicast).

Example

```
Console#show ntp
Polling      : 1024 seconds
Current Mode : unicast
```
Manual Configuration Commands

clock summer-time (date)  This command sets the start, end, and offset times of summer time (daylight savings time) for the switch on a one-time basis. Use the no form to disable summer time.

Syntax

clock summer-time name date b-date b-month b-hour b-minute e-date e-month e-year e-hour e-minute [offset]

no clock summer-time

name - Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-date - Day of the month when summer time will begin. (Range: 1-31)

b-month - The month when summer time will begin. (Options: january | february | march | april | may | june | july | august | september | october | november | december)

b-year - The year summer time will begin.

b-hour - The hour summer time will begin. (Range: 0-23 hours)

b-minute - The minute summer time will begin. (Range: 0-59 minutes)

e-date - Day of the month when summer time will end. (Range: 1-31)

e-month - The month when summer time will end. (Options: january | february | march | april | may | june | july | august | september | october | november | december)

e-year - The year summer time will end.

e-hour - The hour summer time will end. (Range: 0-23 hours)

e-minute - The minute summer time will end. (Range: 0-59 minutes)

offset - Summer time offset from the regular time zone, in minutes. (Range: 30-120 minutes)

Default Setting

Disabled
**Command Mode**
Global Configuration

**Command Usage**
◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

◆ This command sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

**Example**
```
Console(config)#clock summer-time DEST date april 1 2007 23 23 april 23 2007 23 23 60
Console(config)#
```

**Related Commands**
show sntp (144)

clock summer-time (predefined) This command configures the summer time (daylight savings time) status and settings for the switch using predefined configurations for several major regions in the world. Use the no form to disable summer time.

**Syntax**
```
clock summer-time name predefined [australia | europe | new-zealand | usa]
```
```
no clock summer-time
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
This command sets the summer-time time relative to the configured time zone. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time time zone appropriate for your location, or manually configure summer time if these predefined configurations do not apply to your location (see `clock summer-time (date)` or `clock summer-time (recurring)`).

**Example**
The following example sets the Summer Time setting to use the predefined settings for the European region.

```
Console(config)#clock summer-time MESZ predefined europe
```

**Related Commands**
*show sntp (144)*

**clock summer-time (recurring)**
This command allows the user to manually configure the start, end, and offset times of summer time (daylight savings time) for the switch on a recurring basis. Use the `no` form to disable summer-time.

**Syntax**
```
clock summer-time name recurring b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute [offset]
```
```
no clock summer-time
```

- `name` - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- `b-week` - The week of the month when summer time will begin. (Range: 1-5)
- `b-day` - The day of the week when summer time will begin. (Options: `sunday` | `monday` | `tuesday` | `wednesday` | `thursday` | `friday` | `saturday`)
- `e-week` - The week of the month when summer time will end. (Range: 1-5)
- `e-day` - The day of the week when summer time will end. (Options: `sunday` | `monday` | `tuesday` | `wednesday` | `thursday` | `friday` | `saturday`)
- `b-hour` - The hour of the day when summer time will begin. (Range: 0-23)
- `b-minute` - The minute of the hour when summer time will begin. (Range: 0-59)
- `e-hour` - The hour of the day when summer time will end. (Range: 0-23)
- `e-minute` - The minute of the hour when summer time will end. (Range: 0-59)
- `offset` - The offset period from the configured time zone. (Range: 0-23)
**b-month** - The month when summer time will begin. (Options: \texttt{january} | \texttt{february} | \texttt{march} | \texttt{april} | \texttt{may} | \texttt{june} | \texttt{july} | \texttt{august} | \texttt{september} | \texttt{october} | \texttt{november} | \texttt{december})

**b-hour** - The hour when summer time will begin. (Range: 0-23 hours)

**b-minute** - The minute when summer time will begin. (Range: 0-59 minutes)

**e-week** - The week of the month when summer time will end. (Range: 1-5)

**e-day** - The day of the week summer time will end. (Options: \texttt{sunday} | \texttt{monday} | \texttt{tuesday} | \texttt{wednesday} | \texttt{thursday} | \texttt{friday} | \texttt{saturday})

**e-month** - The month when summer time will end. (Options: \texttt{january} | \texttt{february} | \texttt{march} | \texttt{april} | \texttt{may} | \texttt{june} | \texttt{july} | \texttt{august} | \texttt{september} | \texttt{october} | \texttt{november} | \texttt{december})

**e-hour** - The hour when summer time will end. (Range: 0-23 hours)

**e-minute** - The minute when summer time will end. (Range: 0-59 minutes)

**offset** - Summer-time offset from the regular time zone, in minutes. (Range: 30-120 minutes)

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

\begin{itemize}
  \item In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
  \item This command sets the summer-time time zone relative to the currently configured time zone. To display a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone (that is, the offset).
\end{itemize}

**Example**

The following example sets a recurring 60 minute offset summer-time to begin on the Friday of the 1st week of March at 01:59 hours and summer time to end on the Saturday of the 2nd week of November at 01:59 hours.

```
Console(config)#clock summer-time MESZ recurring 1 friday march 01 59 2
  saturday november 1 59 60
Console(config)#
```

**Related Commands**

show sntp (144)
clock timezone  This command sets the time zone for the switch's internal clock.

Syntax

```
clock timezone name hour hours minute minutes
 {before-utc | after-utc}
```

- `name` - Name of timezone, usually an acronym. (Range: 1-30 characters)
- `hour` - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)
- `minutes` - Number of minutes before/after UTC. (Range: 0-59 minutes)
- `before-utc` - Sets the local time zone before (west) of UTC.
- `after-utc` - Sets the local time zone after (east) of UTC.

Default Setting
None

Command Mode
Global Configuration

Command Usage
This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (after) or west (before) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands
show sntp (144)

calendar set  This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

```
calendar set hour min sec (day month year | month day year)
```

- `hour` - Hour in 24-hour format. (Range: 0 - 23)
- `min` - Minute. (Range: 0 - 59)
- `sec` - Second. (Range: 0 - 59)
- `day` - Day of month. (Range: 1 - 31)
**Chapter 4 | System Management Commands**

**Time**

*month* - *january | february | march | april | may | june | july | august | september | october | november | december*

*year* - Year (4-digit). (Range: 1970-2037)

**Default Setting**
None

**Command Mode**
Privileged Exec

**Command Usage**
Note that when SNTP is enabled, the system clock cannot be manually configured.

**Example**
This example shows how to set the system clock to 15:12:34, February 1st, 2012.

```
Console#calendar set 15:12:34 1 February 2012
Console#
```

**show calendar**
This command displays the system clock.

**Default Setting**
None

**Command Mode**
Normal Exec, Privileged Exec

**Example**
```
Console#show calendar
Time Zone : UTC, 00:00
Summer Time : Not configured
Summer Time in Effect : No
Console#
```
**Time Range**

This section describes the commands used to set a time range for use by other functions, such as Access Control Lists.

**Table 24: Time Range Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>time-range</td>
<td>Specifies the name of a time range, and enters time range configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>absolute</td>
<td>Sets the absolute time range for the execution of a command</td>
<td>TR</td>
</tr>
<tr>
<td>periodic</td>
<td>Sets the time range for the periodic execution of a command</td>
<td>TR</td>
</tr>
<tr>
<td>show time-range</td>
<td>Shows configured time ranges.</td>
<td>PE</td>
</tr>
</tbody>
</table>

**Syntax**

```
[no] time-range name

name - Name of the time range. (Range: 1-16 characters)
```

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- This command sets a time range for use by other functions, such as Access Control Lists.
- A maximum of eight rules can be configured for a time range.

**Example**

```
Console(config)#time-range r&d
Console(config-time-range)#
```

**Related Commands**

- Access Control Lists (351)
**absolute**  This command sets the absolute time range for the execution of a command. Use the **no** form to remove a previously specified time.

**Syntax**

```
absolute start hour minute day month year
[end hour minutes day month year]
absolute end hour minutes day month year
no absolute

hour - Hour in 24-hour format. (Range: 0-23)
minute - Minute. (Range: 0-59)
day - Day of month. (Range: 1-31)
month - january | february | march | april | may | june | july | august |
         | september | october | november | december
year - Year (4-digit). (Range: 2013-2037)
```

**Default Setting**

None

**Command Mode**

Time Range Configuration

**Command Usage**

- If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.

- If both an absolute rule and one or more periodic rules are configured for the same time range (e.g., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

**Example**

This example configures the time for the single occurrence of an event.

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april 2009
Console(config-time-range)#
```
**periodic** This command sets the time range for the periodic execution of a command. Use the no form to remove a previously specified time range.

**Syntax**

```plaintext
[no] periodic (daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend) hour minute to (daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend | hour minute)

daily - Daily
friday - Friday
monday - Monday
saturday - Saturday
sunday - Sunday
thursday - Thursday
tuesday - Tuesday
wednesday - Wednesday
weekdays - Weekdays
weekend - Weekends

hours - Hour in 24-hour format. (Range: 0-23)
minutes - Minute. (Range: 0-59)
```

**Default Setting**
None

**Command Mode**
Time Range Configuration

**Command Usage**
- If a time range is already configured, you must use the no form of this command to remove the current entry prior to configuring a new time range.
- If both an absolute rule and one or more periodic rules are configured for the same time range (e.g., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

**Example**
This example configures a time range for the periodic occurrence of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```
**show time-range** This command shows configured time ranges.

**Syntax**

```
show time-range [name]
```

*name* - Name of the time range. (Range: 1-16 characters)

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**

```
Console#show time-range r&d
Time-range r&d:
  absolute start 01:01 01 April 2009
  periodic    Daily 01:01 to    Daily 02:01
  periodic    Daily 02:01 to    Daily 03:01
Console#
```

---

**Switch Clustering**

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

**Table 25: Switch Cluster Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>Configures clustering on the switch</td>
<td>GC</td>
</tr>
<tr>
<td>cluster commander</td>
<td>Configures the switch as a cluster Commander</td>
<td>GC</td>
</tr>
<tr>
<td>cluster ip-pool</td>
<td>Sets the cluster IP address pool for Members</td>
<td>GC</td>
</tr>
<tr>
<td>cluster member</td>
<td>Sets Candidate switches as cluster members</td>
<td>GC</td>
</tr>
<tr>
<td>rcommand</td>
<td>Provides configuration access to Member switches</td>
<td>PE</td>
</tr>
<tr>
<td>show cluster</td>
<td>Displays the switch clustering status</td>
<td>PE</td>
</tr>
<tr>
<td>show cluster members</td>
<td>Displays current cluster Members</td>
<td>PE</td>
</tr>
<tr>
<td>show cluster candidates</td>
<td>Displays current cluster Candidates in the network</td>
<td>PE</td>
</tr>
</tbody>
</table>

**Using Switch Clustering**

- A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the...
Commander through its IP address, and then use the Commander to manage the Member switches through the cluster’s “internal” IP addresses.

◆ Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.

◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

◆ The cluster VLAN 4093 is not configured by default. Before using clustering, take the following actions to set up this VLAN:

1. Create VLAN 4093 (see “Editing VLAN Groups” on page 501).
2. Add the participating ports to this VLAN (see “Configuring VLAN Interfaces” on page 503), and set them to hybrid mode, tagged members, PVID = 1, and acceptable frame type = all.

Note: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the rcommand to connect to the Member switch.

cluster
This command enables clustering on the switch. Use the no form to disable clustering.

Syntax
[no] cluster

Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
◆ To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

◆ Switch clusters are limited to the same Ethernet broadcast domain.
◆ There can be up to 100 candidates and 36 member switches in one cluster.

◆ A switch can only be a Member of one cluster.

◆ Configured switch clusters are maintained across power resets and network changes.

Example

```
Console(config)#cluster
Console(config)#
```

**cluster commander**  This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

**Syntax**

```
[no] cluster commander
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

◆ Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the `rcommand` command to connect to the Member switch.

Example

```
Console(config)#cluster commander
Console(config)#
```
**cluster ip-pool**  This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

**Syntax**

```
cluster ip-pool ip-address
no cluster ip-pool
```

*ip-address* - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

**Default Setting**

10.254.254.1

**Command Mode**

Global Configuration

**Command Usage**

◆ An “internal” IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.

◆ Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

◆ You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

**Example**

```
Console(config)#cluster ip-pool 10.2.3.4
Console(config)#
```

**cluster member**  This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

**Syntax**

```
cluster member mac-address mac-address id member-id
no cluster member id member-id
```

*mac-address* - The MAC address of the Candidate switch.

*member-id* - The ID number to assign to the Member switch. (Range: 1-36)

**Default Setting**

No Members
**Command Mode**
Global Configuration

**Command Usage**
* The maximum number of cluster Members is 36.
* The maximum number of cluster Candidates is 100.

**Example**

```
Console(config)# cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

**rcommand** This command provides access to a cluster Member CLI for configuration.

**Syntax**
```
rcommand id member-id
```

* member-id - The ID number of the Member switch.
  (Range: 1-36)

**Command Mode**
Privileged Exec

**Command Usage**
* This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.
* There is no need to enter the username and password for access to the Member switch CLI.

**Example**

```
Console# rcommand id 1

   CLI session with the EX-3524 is opened.
   To end the CLI session, enter [Exit].

Vty-1#
```
**show cluster**  This command shows the switch clustering configuration.

**Command Mode**  
Privileged Exec

**Example**
```
Console#show cluster
Role : commander
Interval Heartbeat : 30
Heartbeat Loss Count : 3 seconds
Number of Members : 1
Number of Candidates : 2
Console#
```

**show cluster members**  This command shows the current switch cluster members.

**Command Mode**  
Privileged Exec

**Example**
```
Console#show cluster members
Cluster Members:
ID : 1
Role : Active member
IP Address : 10.254.254.2
MAC Address : 00-E0-0C-00-00-FE
Description : EX-3524 Managed POE/POE+ Switch
Console#
```

**show cluster candidates**  This command shows the discovered Candidate switches in the network.

**Command Mode**  
Privileged Exec

**Example**
```
Console#show cluster candidates
Cluster Candidates:
Role MAC Address Description
---------- ------------- -------------------------------
Active member 00-E0-0C-00-00-FE EX-3524 Managed POE/POE+ Switch
CANDIDATE 00-12-CF-0B-47-A0 EX-3524 Managed POE/POE+ Switch
Console#
```
Adopt Device

The EX-3528 and EX-3548 can be managed by a centralized management “Controller,” where the term “Controller” refers to any controller device that is capable of managing these switches. The adopt agent software component runs on the switch in order to facilitate management by remote controller. This component is included in each software release, but can also be upgraded separately via the CLI adoptd upgrade command.

Once the switch has been adopted by a centralized controller, it can receive CLI commands from the controller and send back status messages. Centralized management via SNMP is provided via direct communication between the adopted device agent and the SNMP daemon running on the switch.

Upon adoption, the controller will send the full set of configuration settings (a subset of the switch’s configuration settings) down to the switch. Any configuration settings not supported by the controller will not be overwritten. Subsequent configuration from the controller will result in only the modified commands being pushed down to the switch. Users will be able to directly access the switch’s CLI for configuration. This could result in the switch’s configuration and the controller’s view of the switch’s configuration being out of sync. A re-adoption can be used to force the full configuration to be pushed down to the switch.

The controller will support configuration of a subset of the switch features. This will include but is not limited to:

- Hostname
- Ethernet Port
- Shutdown
- Duplex
- Speed
- VLANs
- IP address
- Static Routes
- PoE
- ACLs (L2/L3/L4)
- QoS Policy
- IGMP Snooping
- Management Policy
  - username/password
  - role
  - ssh
  - http/https
  - snmp
◆ Static Link Aggregation
◆ Port Mirroring
◆ Storm Control
◆ DoS Attacks

The following additional operations can also be executed on the switch from the controller:
◆ Image upgrade
◆ Reload
◆ Tech-support dump
◆ File Management commands
◆ View debug messages stored in /tmp folder
  (adoption_dbg_msg, adoption_dbg_msg_1, adoption_dbg_msg_2)
◆ Debugging options for adoptd (adopted device)

The following commands are supported for the adopted device:

**Table 26: Switch Cluster Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller hello-interval adjacency-hold-time</td>
<td>Sets the hello interval and adjacency hold time</td>
<td>GC</td>
</tr>
<tr>
<td>controller host ip address</td>
<td>Configures up to four controller addresses</td>
<td>GC</td>
</tr>
<tr>
<td>adoptd upgrade</td>
<td>Upgrades the adopt device software</td>
<td>PE</td>
</tr>
<tr>
<td>debug adoption</td>
<td>Enables adopt device debug messages</td>
<td>PE</td>
</tr>
<tr>
<td>no adoption</td>
<td>Restarts the adopt device process</td>
<td>PE</td>
</tr>
<tr>
<td>show adoption debug</td>
<td>Shows adopt device debug messages</td>
<td>PE</td>
</tr>
<tr>
<td>show adoption history</td>
<td>Shows all adopt device related activities since boot up</td>
<td>PE</td>
</tr>
<tr>
<td>show adoption status</td>
<td>Shows adopt device details such as controller IP, adopted time, etc.</td>
<td>PE</td>
</tr>
<tr>
<td>show tech-support</td>
<td>Shows all switch configuration settings and status and adopted device related information</td>
<td>PE</td>
</tr>
<tr>
<td>show version</td>
<td>Shows switch version and adopted device version</td>
<td>PE</td>
</tr>
</tbody>
</table>
Use this command to set the hello interval and adjacency hold time. Use the `no` form to restore the default settings.

**Syntax**

```
controller hello-interval  hello-interval  adjacency-hold-time  hold-time
```

- `hello-interval` - Specifies the interval between sending hello packets to the controller. (Range: 1-120 seconds)
- `hold-time` - The maximum interval after which a controller is declared dead if a keep-alive or update message has not been received. (Range: 2-600 seconds)

**Default Setting**

- `hello-interval`: 15 seconds
- `hold-time`: 46 seconds

**Command Mode**

Global Configuration

**Command Usage**

Use this command to set the timers used for monitoring connectivity to the controllers. These timers will be applied to all configured controllers.

**Example**

```
Console(config)#controller hello-interval 5 adjacency-hold-time 20
Console(config)#
```

Use this command to configure up to four controller addresses. Use the `no` form to remove a controller address.

**Syntax**

```
controller host ip address priority ip-address
```

- `priority` - The priority controls the order in which switch tries to connect with multiple controllers. (Range: 1-4)
- `ip-address` - IPv4 address of a controller.

**Default Setting**

None

**Command Mode**

Global Configuration
Command Usage
When more than one controller address is configured, the switch attempts to connect to the controllers in a round-robin fashion based on the priority settings.

Example

```
Console(config)#controller host ip address 192.168.0.99
Console(config)#
```

adoptd upgrade  Use this command to upgrade the adopt device software.

Syntax

```
adoptd upgrade protocol://server-address[/path]/file
```

- **protocol** - Supported protocols include tftp.
- **server-address** - IPv4 address of the file server.
- **path** - The directory path to the software image.
- **file** - The software image for the adopt device application.

Command Mode
Privileged Exec

Command Usage

- The adoptd component is included in each software release, but can also be upgraded separately using the **adoptd upgrade** command.

- The adoptd image file consists of a header, and then the contents of what is normally a tar.gz file. The header has two md5 checksums, while the tar.gz file includes the adoptd image and a log file which are all be saved in adoptd partition. The image has a the suffix “img”.

- Downloading the adoptd image will restart the system. You will have to reboot the switch to initiate the new image. After the switch restarts, you can view the version number using the **show version** command.

- Note that the length of the adoptd file name may be longer than that permitted by some file servers, in which case you have to shorten the file name.

Example
In the following example, the path is in the default download directory defined on the file server, and is therefore not specified here.

```
Console#adoptd upgrade tftp://192.168.0.99/ex3500-adoptd-5.8.0.0.img
Flash programming started
Flash programming completed
Success
```
debug adoption  Use this command to enable adopt device (adoptd) debug messages. Use the no form to disable adoptd debug messages.

Syntax

[no] debug adoption

Default Setting

Enabled

Command Mode

Privileged Exec

Example

Console#debug adoption
Console#

no adoption  Use this command to restart the adopt device process.

Syntax

no adoption

Command Mode

Privileged Exec

Command Usage

This command will disconnect the adopted device from any configured controllers, and then restarts the adoption process.

Example

Console#no adoption
Console#

show adoption debug  Use this command to show adopt device (adoptd) debug messages.

Syntax

show adoption debug
Command Mode
Privileged Exec

Command Usage
Message format for each entry includes a time stamp and event similar to that shown below.

2014-05-08 20:11:01: Unadopted,
2014-05-08 19:15:16: Adopted by 192.168.100.67,

Example

Console# show adoption debug
[2014-12-02 02:25:48] vendor_record_pid: pid 332
[2014-12-02 02:25:48] vendor_init:
[2014-12-02 02:25:48] vendor_init: SW version is ‘5.8.0.0-209434X’
[2014-12-02 02:25:48] vendor_init: vendor init complete
[2014-12-02 02:25:48] snmpp_init:
[2014-12-02 02:25:48] snmpp_init: Initialize snmp mutex
[2014-12-02 02:25:48] main: Waiting for adopter address(es) to be configured...
[2014-12-02 02:26:35] vendor_read_config_file: Configured adopter 1 =‘192.168.0.1’
[2014-12-02 02:26:35] vendor_read_config_file: Possible adopter[0] =’192.168.0.1’
[2014-12-02 02:26:35] main: Delay start by 15 seconds
[2014-12-02 02:26:50] main: Create the websocket context
[2014-12-02 02:26:50] Initial logging level 287
...
...

show adoption history

Use this command to show all adopt device related activities since boot up.

Syntax

show adoption history

Command Mode
Privileged Exec

Command Usage
Message format for each entry includes a time stamp and event similar to that shown below.

2014-05-08 20:11:01: Unadopted,
2014-05-08 19:15:16: Adopted by 192.168.100.67,

Example

Console# show adoption history
2014-12-02 02:26:57: Adopted by 192.168.0.1
Console#
**show adoption status**  Use this command to show adopt device details such as controller IP, adopted time, etc.

**Syntax**

```
show adoption status
```

**Command Mode**
Privileged Exec

**Example**

```
Console#show adoption status
Adopted by:
192.168.0.1
Console#
```
SNMP commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 27: SNMP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General SNMP Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>snmp-server</td>
<td>Enables the SNMP agent</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server community</td>
<td>Sets up the community access string to permit access to SNMP commands</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server contact</td>
<td>Sets the system contact string</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server location</td>
<td>Sets the system location string</td>
<td>GC</td>
</tr>
<tr>
<td>show snmp</td>
<td>Displays the status of SNMP communications</td>
<td>NE, PE</td>
</tr>
<tr>
<td><strong>SNMP Target Host Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>Enables the device to send SNMP traps (i.e., SNMP notifications)</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server host</td>
<td>Specifies the recipient of an SNMP notification operation</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server enable port-traps</td>
<td>Enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed</td>
<td>IC</td>
</tr>
<tr>
<td>mac-notification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show snmp-server enable port-traps</td>
<td>Shows if SNMP traps are enabled or disabled for the specified interfaces</td>
<td>PE</td>
</tr>
<tr>
<td><strong>SNMPv3 Engine Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>snmp-server engine-id</td>
<td>Sets the SNMP engine ID</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server group</td>
<td>Adds an SNMP group, mapping users to views</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server user</td>
<td>Adds a user to an SNMP group</td>
<td>GC</td>
</tr>
<tr>
<td>snmp-server view</td>
<td>Adds an SNMP view</td>
<td>GC</td>
</tr>
<tr>
<td>show snmp engine-id</td>
<td>Shows the SNMP engine ID</td>
<td>PE</td>
</tr>
<tr>
<td>show snmp group</td>
<td>Shows the SNMP groups</td>
<td>PE</td>
</tr>
</tbody>
</table>
### Table 27: SNMP Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp user</td>
<td>Shows the SNMP users</td>
<td>PE</td>
</tr>
<tr>
<td>show snmp view</td>
<td>Shows the SNMP views</td>
<td>PE</td>
</tr>
</tbody>
</table>

### Notification Log Commands

- **nlm**: Enables the specified notification log
- **snmp-server notify-filter**: Creates a notification log and specifies the target host
- **show nlm oper-status**: Shows operation status of configured notification logs
- **show snmp notify-filter**: Displays the configured notification logs

### ATC Trap Commands

- **snmp-server enable port-traps atc broadcast-alarm-clear**: Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered
- **snmp-server enable port-traps atc broadcast-alarm-fire**: Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control
- **snmp-server enable port-traps atc broadcast-control-apply**: Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires
- **snmp-server enable port-traps atc broadcast-control-release**: Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires
- **snmp-server enable port-traps atc multicast-alarm-clear**: Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered
- **snmp-server enable port-traps atc multicast-alarm-fire**: Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control
- **snmp-server enable port-traps atc multicast-control-apply**: Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires
- **snmp-server enable port-traps atc multicast-control-release**: Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires

### Transceiver Power Threshold Trap Commands

- **transceiver-threshold current**: Sends a trap when the transceiver current falls outside the specified thresholds
- **transceiver-threshold rx-power**: Sends a trap when the power level of the received signal falls outside the specified thresholds
- **transceiver-threshold temperature**: Sends a trap when the transceiver temperature falls outside the specified thresholds
- **transceiver-threshold tx-power**: Sends a trap when the power level of the transmitted signal power outside the specified thresholds
- **transceiver-threshold voltage**: Sends a trap when the transceiver voltage falls outside the specified thresholds
**General SNMP Commands**

**snmp-server**

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

**Syntax**

```plaintext
[no] snmp-server
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Example**

```plaintext
Console(config)#snmp-server
Console(config)#
```

**snmp-server community**

This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

**Syntax**

```plaintext
snmp-server community string [ro | rw]
no snmp-server community string
```

- **string** - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

---

**Table 27: SNMP Commands (Continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Sets the rising and falling threshold for the memory utilization alarm</td>
<td>GC</td>
</tr>
<tr>
<td>process cpu</td>
<td>Sets the rising and falling threshold for the CPU utilization alarm</td>
<td>GC</td>
</tr>
<tr>
<td>show memory</td>
<td>Shows memory utilization parameters</td>
<td>PE</td>
</tr>
<tr>
<td>show process cpu</td>
<td>Shows CPU utilization parameters</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

**Additional Trap Commands**

- **memory**
- **process cpu**
- **show memory**
- **show process cpu**
Default Setting
◆ public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
◆ private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode
Global Configuration

Example
```
Console(config)#snmp-server community alpha rw
Console(config)#
```

**snmp-server contact**
This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax
```
snmp-server contact string
no snmp-server contact
```

- **string** - String that describes the system contact information.
  (Maximum length: 255 characters)

Default Setting
None

Command Mode
Global Configuration

Example
```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands
**snmp-server location** (175)
**snmp-server location**  This command sets the system location string. Use the no form to remove the location string.

**Syntax**

```plaintext
snmp-server location text
no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)
```

**Default Setting**

None

**Command Mode**

Global Configuration

**Example**

```plaintext
Console(config)#snmp-server location WC-19
Console(config)#
```

**Related Commands**

`snmp-server contact (174)`

---

**show snmp**  This command can be used to check the status of SNMP communications.

**Default Setting**

None

**Command Mode**

Normal Exec, Privileged Exec

**Command Usage**

This command provides information on the community access strings, counters for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the `snmp-server enable traps` command.

**Example**

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
Authentication : Enabled
Link-up-down : Enabled
MAC-notification : Disabled
MAC-notification interval : 1 second(s)
```
SNMP Communities:
1. public, and the access level is read-only
2. private, and the access level is read/write

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP Logging: Disabled
Console#

SNMP Target Host Commands

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the no form to disable SNMP notifications.

Syntax

[no] snmp-server enable traps [authentication | link-up-down | mac-notification [interval seconds]]

  authentication - Keyword to issue authentication failure notifications.
  link-up-down - Keyword to issue link-up or link-down notifications.
  mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

  interval - Specifies the interval between issuing two consecutive traps. (Range: 1-3600 seconds; Default: 1 second)

Default Setting
Issue authentication and link-up-down traps.
Other traps are disabled.

Command Mode
Global Configuration

Command Usage
- If you do not enter an snmp-server enable traps command, no notifications controlled by this command are sent. In order to configure this device to send
SNMP notifications, you must enter at least one `snmp-server enable traps` command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

◆ The `snmp-server enable traps` command is used in conjunction with the `snmp-server host` command. Use the `snmp-server host` command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one `snmp-server host` command.

◆ The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the `snmp-server group` command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

`snmp-server host (177)`

**snmp-server host**  This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the `no` form to remove the specified host.

**Syntax**

```
snmp-server host host-addr [inform [retry retries | timeout seconds]]
community-string
[version {1 | 2c | 3 {auth | noauth | priv} [udp-port port]]

no snmp-server host host-addr
```

- `host-addr` - IPv4 or IPv6 address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- `inform` - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
- `retry` - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- `timeout` - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- `community-string` - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the `snmp-server host` command by itself, we recommend defining it with the `snmp-server community` command prior to using the `snmp-server host` command. (Maximum length: 32 characters)
version - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

auth | noauth | priv - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” in the System Reference Guide for further information about these authentication and encryption options.

port - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting
Host Address: None
Notification Type: Traps
SNMP Version: 1
UDP Port: 162

Command Mode
Global Configuration

Command Usage
◆ If you do not enter an snmp-server host command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server host command. In order to enable multiple hosts, you must issue a separate snmp-server host command for each host.

◆ The snmp-server host command is used in conjunction with the snmp-server enable traps command. Use the snmp-server enable traps command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one snmp-server enable traps command and the snmp-server host command for that host must be enabled.

◆ Some notification types cannot be controlled with the snmp-server enable traps command. For example, some notification types are always enabled.

◆ Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:
1. Enable the SNMP agent (page 173).
2. Create a view with the required notification messages (page 185).
3. Create a group that includes the required notify view (page 182).
4. Allow the switch to send SNMP traps; i.e., notifications (page 176).
5. Specify the target host that will receive inform messages with the `snmp-server host` command as described in this section.

To send an inform to a SNMPv3 host, complete these steps:
1. Enable the SNMP agent (page 173).
2. Create a remote SNMPv3 user to use in the message exchange process (page 183).
3. Create a view with the required notification messages (page 185).
4. Create a group that includes the required notify view (page 182).
5. Allow the switch to send SNMP traps; i.e., notifications (page 176).
6. Specify the target host that will receive inform messages with the `snmp-server host` command as described in this section.

◆ The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the `snmp-server host` command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

◆ If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the `snmp-server user` command. Otherwise, an SNMPv3 group will be automatically created by the `snmp-server host` command using the name of the specified community string, and default settings for the read, write, and notify view.

**Example**

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

**Related Commands**

`snmp-server enable traps (176)`

```
**snmp-server enable port-traps**
```

This command enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed. Use the no form to restore the default setting.

**Syntax**

```
[no] snmp-server enable port-traps mac-notification
```

**mac-notification** - Keyword to issue trap when a dynamic MAC address is added or removed.

**Default Setting**

Disabled
**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
This command can enable MAC authentication traps on the current interface only if they are also enabled at the global level with the `snmp-server enable traps mac-authentication` command.

**Example**
```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config)#
```

**show snmp-server enable port-traps**
This command shows if SNMP traps are enabled or disabled for the specified interfaces.

**Syntax**
```
show snmp-server enable port-traps interface [interface]
interface
```

- `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)

- `port-channel channel-id` (Range: 1-16)

**Command Mode**
Privileged Exec

**Example**
```
Console#show snmp-server enable port-traps interface
Interface MAC Notification Trap
---------- ---------------------
Eth 1/1 No
Eth 1/2 No
Eth 1/3 No
:
```
SNMPv3 Commands

**snmp-server engine-id**

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

**Syntax**

```
snmp-server engine-id {local | remote {ip-address}} engineid-string
no snmp-server engine-id {local | remote {ip-address}}
```

- **local** - Specifies the SNMP engine on this switch.
- **remote** - Specifies an SNMP engine on a remote device.
- **ip-address** - IPv4 address of the remote device.
- **engineid-string** - String identifying the engine ID. (Range: 9-64 hexadecimal characters)

**Default Setting**

A unique engine ID is automatically generated by the switch based on its MAC address.

**Command Mode**

Global Configuration

**Command Usage**

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

- A remote engine ID is required when using SNMPv3 informs. (See the **snmp-server host** command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it.

- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value “0123456789” is equivalent to “0123456789” followed by 16 zeroes for a local engine ID.

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 183).
Example

```console
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#
```

Related Commands

**snmp-server host (177)**

**snmp-server group** This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

**Syntax**

```plaintext
snmp-server group groupname
    {v1 | v2c | v3 [auth | noauth | priv]}
    [read readview] [write writeview] [notify notifyview]
```

```plaintext
no snmp-server group groupname
```

- **groupname** - Name of an SNMP group. (Range: 1-32 characters)
- **v1 | v2c | v3** - Use SNMP version 1, 2c or 3.
- **auth | noauth | priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” in the System Reference Guide for further information about these authentication and encryption options.
- **readview** - Defines the view for read access. (1-32 characters)
- **writeview** - Defines the view for write access. (1-32 characters)
- **notifyview** - Defines the view for notifications. (1-32 characters)

**Default Setting**

Default groups: public\(^1\) (read only), private\(^2\) (read/write)

- **readview** - Every object belonging to the Internet OID space (1).
- **writeview** - Nothing is defined.
- **notifyview** - Nothing is defined.

**Command Mode**

Global Configuration

**Command Usage**

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the **snmp-server user** command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.

---

1. No view is defined.
2. Maps to the defaultview.
◆ For additional information on the notification messages supported by this switch, see the table for “Supported Notification Messages” in the System Reference Guide. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the snmp-server enable traps command.

**Example**

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

**snmp-server user**  
This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the no form to remove a user from an SNMP group.

**Syntax**

```
snmp-server user username groupname
    {v1 | v2c | v3 [encrypted]} [auth {md5 | sha} auth-password [priv {3des | aes128 | aes192 | aes256 | des56} priv-password]]

snmp-server user username groupname remote ip-address
    {v3 [encrypted]} [auth {md5 | sha} auth-password [priv {3des | aes128 | aes192 | aes256 | des56} priv-password]]

no snmp-server user username {v1 | v2c | v3 | remote ip-address v3}
```

- **username** - Name of user connecting to the SNMP agent.  
  (Range: 1-32 characters)
- **groupname** - Name of an SNMP group to which the user is assigned.  
  (Range: 1-32 characters)
- **remote** - Specifies an SNMP engine on a remote device.
- **ip-address** - IPv4 address of the remote device.
- **v1 | v2c | v3** - Use SNMP version 1, 2c or 3.
- **encrypted** - Accepts the password as encrypted input.
- **auth** - Uses SNMPv3 with authentication.
- **md5 | sha** - Uses MD5 or SHA authentication.
- **auth-password** - Authentication password. Enter as plain text if the encrypted option is not used. Otherwise, enter an encrypted password.  
  (Range: 8-32 characters for unencrypted password)

If the encrypted option is selected, enter an encrypted password.  
(Range: 32 characters for MD5 encrypted password, 40 characters for SHA encrypted password)
- **3des** - Uses SNMPv3 with privacy with 3DES (168-bit) encryption.
- **aes128** - Uses SNMPv3 with privacy with AES128 encryption.
**aes192** - Uses SNMPv3 with privacy with AES192 encryption.

**aes256** - Uses SNMPv3 with privacy with AES256 encryption.

**des56** - Uses SNMPv3 with privacy with DES56 encryption.

**priv-password** - Privacy password. Enter as plain text if the encrypted option is not used. Otherwise, enter an encrypted password. (Range: 8-32 characters)

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.

- Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the `snmp-server engine-id` command before using this configuration command.

- Before you configure a remote user, use the `snmp-server engine-id` command to specify the engine ID for the remote device where the user resides. Then use the `snmp-server user` command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the `snmp-server user` command specifying a remote user will fail.

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it.

**Example**

```
Console(config)#snmp-server user steve r&d v3 auth md5 greenpeace priv des56 einstien
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#snmp-server user mark r&d remote 192.168.1.19 v3 auth md5
greenpeace priv des56 einstien
Console(config)#
```
snmp-server view  This command adds an SNMP view which controls user access to the MIB. Use the `no` form to remove an SNMP view.

Syntax

```
snmp-server view view-name oid-tree {included | excluded}
```

```
no snmp-server view view-name
```

`view-name` - Name of an SNMP view. (Range: 1-32 characters)

`oid-tree` - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

`included` - Defines an included view.

`excluded` - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

◆ Views are used in the `snmp-server group` command to restrict user access to specified portions of the MIB tree.

◆ The predefined view “defaultview” includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.1.1.* included
Console(config)#
```
**show snmp engine-id**

This command shows the SNMP engine ID.

**Command Mode**

Privileged Exec

**Example**

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP Engine ID    : 8000018403FC0A81B7C7E00000
Local SNMP Engine Boots : 29
Remote SNMP Engine ID                                        IP address
80000000030004e2b316c54321                                   192.168.1.19
Console#
```

**Table 28: show snmp engine-id - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local SNMP engineID</td>
<td>String identifying the engine ID.</td>
</tr>
<tr>
<td>Local SNMP engineBoots</td>
<td>The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.</td>
</tr>
<tr>
<td>Remote SNMP engineID</td>
<td>String identifying an engine ID on a remote device.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the device containing the corresponding remote SNMP engine.</td>
</tr>
</tbody>
</table>

**show snmp group**

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

**Command Mode**

Privileged Exec

**Example**

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
```
Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Table 29: show snmp group - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of an SNMP group.</td>
</tr>
<tr>
<td>Security Model</td>
<td>The SNMP version.</td>
</tr>
<tr>
<td>Read View</td>
<td>The associated read view.</td>
</tr>
<tr>
<td>Write View</td>
<td>The associated write view.</td>
</tr>
<tr>
<td>Notify View</td>
<td>The associated notify view.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>The storage type for this entry.</td>
</tr>
<tr>
<td>Row Status</td>
<td>The row status of this entry.</td>
</tr>
</tbody>
</table>

**show snmp user**  
This command shows information on SNMP users.

**Command Mode**  
Privileged Exec

**Example**

```bash
Console# show snmp user
Engine ID : 8000018403fc0a81b7c7e00000
User Name : steve
Group Name : r&d
Security Model : v3
Security Level : Authentication and privacy
Authentication Protocol : MD5
Privacy Protocol : DES56
Storage Type : Nonvolatile
```
Table 30: show snmp user - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine ID</td>
<td>String identifying the engine ID.</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of user connecting to the SNMP agent.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Name of an SNMP group.</td>
</tr>
<tr>
<td>Security Model</td>
<td>Shows the SNMP version 1, 2c or 3.</td>
</tr>
<tr>
<td>Security Level</td>
<td>Shows if authentication or privacy is used.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>The authentication protocol used with SNMPv3.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>The privacy protocol used with SNMPv3.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>The storage type for this entry.</td>
</tr>
<tr>
<td>Row Status</td>
<td>The row status of this entry.</td>
</tr>
<tr>
<td>SNMP remote user</td>
<td>A user associated with an SNMP engine on a remote device.</td>
</tr>
</tbody>
</table>

show snmp view This command shows information on the SNMP views.

Command Mode
Privileged Exec

Example

```
Console#show snmp view
View Name: mib-2
Subtree OID : 1.2.2.3.6.2.1
View Type   : included
Storage Type: permanent
Row Status  : active

View Name   : defaultview
Subtree OID : 1
View Type   : included
Storage Type: volatile
Row Status  : active

Console#
```
Table 31: show snmp view - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Name</td>
<td>Name of an SNMP view.</td>
</tr>
<tr>
<td>Subtree OID</td>
<td>A branch in the MIB tree.</td>
</tr>
<tr>
<td>View Type</td>
<td>Indicates if the view is included or excluded.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>The storage type for this entry.</td>
</tr>
<tr>
<td>Row Status</td>
<td>The row status of this entry.</td>
</tr>
</tbody>
</table>

**Notification Log Commands**

**nlm**  This command enables or disables the specified notification log.

**Syntax**

```
[no] nlm filter-name
```

*filter-name* - Notification log name. (Range: 1-32 characters)

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- Notification logging is enabled by default, but will not start recording information until a logging profile specified by the `snmp-server notify-filter` command is enabled by the `nlm` command.

- Disabling logging with this command does not delete the entries stored in the notification log.

**Example**

This example enables the notification log A1.

```
Console(config)# nlm A1
Console(config)#
```
**snmp-server notify-filter**

This command creates an SNMP notification log. Use the `no` form to remove this log.

**Syntax**

```
[no] snmp-server notify-filter profile-name remote ip-address
```

- `profile-name`: Notification log profile name. (Range: 1-64 characters)
- `ip-address`: IPv4 or IPv6 address of a remote device. The specified target host must already have been configured using the `snmp-server host` command.

**Note:** The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether there are Traps or Informs that may exceed retransmission limits. The Notification Log MIB (NLM, RFC 3014) provides an infrastructure in which information from other MIBs may be logged.

- Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.

- If notification logging is not configured and enabled, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.

- To avoid this problem, notification logging should be configured and enabled using the `snmp-server notify-filter` command and `nlm` command, and these commands stored in the startup configuration file. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.

- When this command is executed, a notification log is created (with the default parameters defined in RFC 3014). Notification logging is enabled by default (see the `nlm` command), but will not start recording information until a logging profile specified with this command is enabled with the `nlm` command.

- Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information
recorded in a notification log, and the entry aging time can only be configured using SNMP from a network management station.

◆ When a trap host is created with the `snmp-server host` command, a default notify filter will be created as shown in the example under the `show snmp notify-filter` command.

**Example**
This example first creates an entry for a remote host, and then instructs the switch to record this device as the remote host for the specified notification log.

```plaintext
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

**show nlm oper-status**
This command shows the operational status of configured notification logs.

**Command Mode**
Privileged Exec

**Example**

```plaintext
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

**show snmp notify-filter**
This command displays the configured notification logs.

**Command Mode**
Privileged Exec

**Example**
This example displays the configured notification logs and associated target hosts.

```
Console#show snmp notify-filter
Filter profile name       IP address
-------------------------  ---------------
A1                        10.1.19.23
Console#
```
Additional Trap Commands

memory  This command sets an SNMP trap based on configured thresholds for memory utilization. Use the no form to restore the default setting.

Syntax

```
memory {rising rising-threshold | falling falling-threshold}
no memory {rising | falling}
```

- `rising-threshold` - Rising threshold for memory utilization alarm expressed in percentage. (Range: 1-100)
- `falling-threshold` - Falling threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

Default Setting
Rising Threshold: 95%
Falling Threshold: 90%

Command Mode
Global Configuration

Command Usage
Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

```
Console(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

Related Commands
show memory (100)

process cpu  This command sets an SNMP trap based on configured thresholds for CPU utilization. Use the no form to restore the default setting.

Syntax

```
process cpu {rising rising-threshold | falling falling-threshold}
no process cpu {rising | falling}
```

- `rising-threshold` - Rising threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)
- `falling-threshold` - Falling threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)
**Default Setting**
Rising Threshold: 90%
Falling Threshold: 70%

**Command Mode**
Global Configuration

**Command Usage**
Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

**Example**
```console
Console(config)#process cpu rising 80
Console(config)#process cpu falling 60
Console#
```

**Related Commands**
`show process cpu (100)`
Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

Table 32: RMON Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon alarm</td>
<td>Sets threshold bounds for a monitored variable</td>
<td>GC</td>
</tr>
<tr>
<td>rmon event</td>
<td>Creates a response event for an alarm</td>
<td>GC</td>
</tr>
<tr>
<td>rmon collection history</td>
<td>Periodically samples statistics</td>
<td>IC</td>
</tr>
<tr>
<td>rmon collection rmon1</td>
<td>Enables statistics collection</td>
<td>IC</td>
</tr>
<tr>
<td>show rmon alarms</td>
<td>Shows the settings for all configured alarms</td>
<td>PE</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Shows the settings for all configured events</td>
<td>PE</td>
</tr>
<tr>
<td>show rmon history</td>
<td>Shows the sampling parameters for each entry</td>
<td>PE</td>
</tr>
<tr>
<td>show rmon statistics</td>
<td>Shows the collected statistics</td>
<td>PE</td>
</tr>
</tbody>
</table>
**rmon alarm**  This command sets threshold bounds for a monitored variable. Use the **no** form to remove an alarm.

**Syntax**

```
rmon alarm index variable interval [absolute | delta] rising-threshold threshold [event-index] falling-threshold threshold [event-index] [owner name]
```

**no rmon alarm**  

```
index
```

- **index** – Index to this entry. (Range: 1-65535)
- **variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.
- **interval** – The polling interval. (Range: 1-31622400 seconds)
- **absolute** – The variable is compared directly to the thresholds at the end of the sampling period.
- **delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.
- **threshold** – An alarm threshold for the sampled variable. (Range: 0-2147483647)
- **event-index** – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)
- **name** – Name of the person who created this entry. (Range: 1-32 characters)

**Default Setting**

1.3.6.1.2.1.16.1.1.6.1 - 1.3.6.1.2.1.16.1.1.6.28/52
Taking delta samples every 30 seconds,
Rising threshold is 892800, assigned to event 0
Falling threshold is 446400, assigned to event 0

**Command Mode**

Global Configuration

**Command Usage**

- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.

- If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be
generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.

◆ If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.

Example

<table>
<thead>
<tr>
<th>Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta rising-threshold 100 1 falling-threshold 30 1 owner mike</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console(config)#</td>
</tr>
</tbody>
</table>

rmon event This command creates a response event for an alarm. Use the no form to remove an event.

Syntax

```plaintext
rmon event index [log] | [trap community] | [description string] | [owner name]
```

```plaintext
no rmon event index
```

index – Index to this entry. (Range: 1-65535)

log – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see “Event Logging” on page 131).

trap – Sends a trap message to all configured trap managers (see “snmp-server host” on page 177).

community – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the rmon event command by itself, it is recommended that the string be defined using the snmp-server community command prior to using the rmon event command. (Range: 1-127 characters)

string – A comment that describes this event. (Range: 1-32 characters)

name – Name of the person who created this entry. (Range: 1-32 characters)

Default Setting
None

Command Mode
Global Configuration
Command Usage
◆ If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.

◆ The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

Example
```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history This command periodically samples statistics on a physical interface. Use the no form to disable periodic sampling.

Syntax
```
rmon collection history controlEntry index
    [buckets number [interval seconds]] |
    [interval seconds] |
    [owner name [buckets number [interval seconds]]]
no rmon collection history controlEntry index
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Index to this entry. (Range: 1-65535)</td>
</tr>
<tr>
<td>number</td>
<td>The number of buckets requested for this entry. (Range: 1-65535)</td>
</tr>
<tr>
<td>seconds</td>
<td>The polling interval. (Range: 1-3600 seconds)</td>
</tr>
<tr>
<td>name</td>
<td>Name of the person who created this entry. (Range: 1-32 characters)</td>
</tr>
</tbody>
</table>

Default Setting
```
1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28/52
Buckets: 8
Interval: 30 seconds for even numbered entries,
1800 seconds for odd numbered entries.
```

Command Mode
Interface Configuration (Ethernet)

Command Usage
◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.

◆ If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
◆ The information collected for each sample includes:
  input octets, packets, broadcast packets, multicast packets, undersize packets,
  oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop
  events, and network utilization.

◆ The switch reserves two controlEntry index entries for each port. If a default
  index entry is re-assigned to another port by this command, the show running-
  config command will display a message indicating that this index is not
  available for the port to which it is normally assigned.

  For example, if control entry 15 is assigned to port 5 as shown below, the show
  running-config command will indicate that this entry is not available for port 8.

  Console(config)#interface ethernet 1/5
  Console(config-if)#rmon collection history controlEntry 15
  Console(config-if)#end
  Console#show running-config
  !
  interface ethernet 1/5
  rmon collection history controlEntry 15 buckets 50 interval 1800
  ...
  interface ethernet 1/8
  no rmon collection history controlEntry 15

Example

| Console(config)#interface ethernet 1/1 |
| Console(config-if)#rmon collection history controlEntry 21 owner mike buckets 24 interval 60 owner mike |
| Console(config-if)# |

rmon collection rmon1

This command enables the collection of statistics on a physical interface. Use the
no form to disable statistics collection.

Syntax

rmon collection rmon1 controlEntry index [owner name]

no rmon collection rmon1 controlEntry index

index – Index to this entry. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-32
characters)

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

◆ By default, each index number equates to a port on the switch, but can be
  changed to any number not currently in use.
◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

◆ The information collected for each entry includes:
  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

**Example**
```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike
Console(config-if)#
```

**show rmon alarms** This command shows the settings for all configured alarms.

**Command Mode**
Privileged Exec

**Example**
```
Console#show rmon alarms
Alarm 1 is valid, owned by
  Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
  Taking delta samples, last value was 0
  Rising threshold is 892800, assigned to event 0
  Falling threshold is 446400, assigned to event 0
  .
```

**show rmon events** This command shows the settings for all configured events.

**Command Mode**
Privileged Exec

**Example**
```
Console#show rmon events
Event 2 is valid, owned by mike
  Description is urgent
  Event firing causes log and trap to community, last fired 00:00:00
Console#
```

**show rmon history** This command shows the sampling parameters configured for each entry in the history group.

**Command Mode**
Privileged Exec
Example

```console
Console#show rmon history
Entry 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.1.1.1 every 1800 seconds
Requested # of time intervals, ie buckets, is 8
Granted # of time intervals, ie buckets, is 8
Sample # 1 began measuring at 00:00:01
Received 77671 octets, 1077 packets,
61 broadcast and 978 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers packets,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Network utilization is estimated at 0
```

show rmon statistics  This command shows the information collected for all configured entries in the statistics group.

Command Mode
Privileged Exec

Example

```console
Console#show rmon statistics
Interface 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.1.1.1 which has
Received 164289 octets, 2372 packets,
120 broadcast and 2211 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events (due to lack of resources): 0
# of packets received of length (in octets):
   64: 2245, 65-127: 87, 128-255: 31,
   256-511: 5, 512-1023: 2, 1024-1518: 2
```
Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access\(^3\) to the data ports.

Table 33: Authentication Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts and Privilege Levels</td>
<td>Configures the basic user names and passwords for management access, and assigns a privilege level to specified command groups or individual commands</td>
</tr>
<tr>
<td>Authentication Sequence</td>
<td>Defines logon authentication method and precedence</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>Configures settings for authentication via a RADIUS server</td>
</tr>
<tr>
<td>TACACS+ Client</td>
<td>Configures settings for authentication via a TACACS+ server</td>
</tr>
<tr>
<td>AAA</td>
<td>Configures authentication, authorization, and accounting for network access</td>
</tr>
<tr>
<td>Web Server</td>
<td>Enables management access via a web browser</td>
</tr>
<tr>
<td>Telnet Server</td>
<td>Enables management access via Telnet</td>
</tr>
<tr>
<td>Secure Shell</td>
<td>Provides secure replacement for Telnet</td>
</tr>
<tr>
<td>802.1X Port Authentication</td>
<td>Configures host authentication on specific ports using 802.1X</td>
</tr>
<tr>
<td>Management IP Filter</td>
<td>Configures IP addresses that are allowed management access</td>
</tr>
<tr>
<td>PPPoE Intermediate Agent</td>
<td>Configures relay parameters required for sending authentication messages between a client and broadband remote access servers</td>
</tr>
</tbody>
</table>

\(^3\) For other methods of controlling client access, see “General Security Measures” on page 271.
Chapter 7 | Authentication Commands
User Accounts and Privilege Levels

User Accounts and Privilege Levels

The basic commands required for management access and assigning command privilege levels are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 120), user authentication via a remote authentication server (page 203), and host access authentication for specific ports (page 244).

Table 34: User Access Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable password</td>
<td>Sets a password to control access to the Privileged Exec level</td>
<td>GC</td>
</tr>
<tr>
<td>username</td>
<td>Establishes a user name-based authentication system at login</td>
<td>GC</td>
</tr>
<tr>
<td>privilege</td>
<td>Assigns a privilege level to specified command groups or individual commands</td>
<td>GC</td>
</tr>
<tr>
<td>show privilege</td>
<td>Shows the privilege level for the current user, or the privilege level for commands modified by the privilege command</td>
<td>PE</td>
</tr>
</tbody>
</table>

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the no form to reset the default password.

Syntax

```
enable password [level level] {0 | 7} password
no enable password [level level]
```

level level - Sets the command access privileges. (Range: 0-15)

Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

Level 0-7 provide the same default access privileges, all within Normal Exec mode under the “Console>” command prompt.

Level 8-14 provide the same default access privileges, including additional commands in Normal Exec mode, and a subset of commands in Privileged Exec mode under the “Console#” command prompt.

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the privilege command.

{0 | 7} - 0 means plain password, 7 means encrypted password.

password - Password for this privilege level. (Maximum length: 32 characters plain text or encrypted, case sensitive)
**Default Setting**
The default is level 15.
The default password is “super”

**Command Mode**
Global Configuration

**Command Usage**
- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the `enable` command.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP server. There is no need for you to manually configure encrypted passwords.

**Example**

```
Console(config)#enable password level 15 0 admin123
Console(config)#
```

**Related Commands**
- `enable (91)`
- `authentication enable (208)`

**username**
This command adds named users, requires authentication at login, specifies or changes a user’s password (or specify that no password is required), or specifies or changes a user’s access level. Use the `no` form to remove a user name.

**Syntax**

```
username name
```

```
no username name
```

- `name` - The name of the user. (Maximum length: 32 characters, case sensitive. Maximum users: 16)

The device has two predefined users, `guest` which is assigned privilege level 0 (Normal Exec) and has access to a limited number of commands, and `admin` which is assigned privilege level 15 and has full access to all commands.

- `access-level level` - Specifies command access privileges. (Range: 0-15)

  Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

  Level 0-7 provide the same default access privileges, all within Normal Exec mode under the “Console>” command prompt.
Level 8-14 provide the same default access privileges, including additional commands in Normal Exec mode, and a subset of commands in Privileged Exec mode under the “Console#” command prompt.

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the `privilege` command.

Any privilege level can access all of the commands assigned to lower privilege levels. For example, privilege level 8 can access all commands assigned to privilege levels 7-0 according to default settings, and to any other commands assigned to levels 7-0 using the `privilege` command.

- `nopassword` - No password is required for this user to log in.
- `{0 | 7}` - 0 means plain password, 7 means encrypted password.
- `password` - The authentication password for the user.

(Maximum length: 32 characters plain text or encrypted, case sensitive)

**Default Setting**
The default access level is Normal Exec.
The factory defaults for the user names and passwords are:

**Table 35: Default Login Settings**

<table>
<thead>
<tr>
<th>username</th>
<th>access-level</th>
<th>password</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest</td>
<td>0</td>
<td>guest</td>
</tr>
<tr>
<td>admin</td>
<td>15</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Command Usage**
The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP server. There is no need for you to manually configure encrypted passwords.

**Example**
This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```
**privilege**  This command assigns a privilege level to specified command groups or individual commands. Use the `no` form to restore the default setting.

**Syntax**

```
privilege mode [all] level level command
no privilege mode [all] command
```

*mode* - The configuration mode containing the specified *command*.  
(See “Understanding Command Modes” on page 82 and “Configuration Commands” on page 83.)

*all* - Modifies the privilege level for all subcommands under the specified *command*.

*level level* - Specifies the privilege level for the specified *command*. Refer to the default settings described for the access level parameter under the *username* command.  (Range: 0-15)

*command* - Specifies any command contained within the specified *mode*.

**Default Setting**

Privilege level 0 provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Level 8 provides access to all display status and configuration commands, except for those controlling various authentication and security features. Level 15 provides full access to all commands.

**Command Mode**

Global Configuration

**Example**

This example sets the privilege level for the ping command to Privileged Exec.

```
Console(config)#privilege exec level 15 ping
Console(config)#
```

**show privilege**  This command shows the privilege level for the current user, or the privilege level for commands modified by the *privilege* command.

**Syntax**

```
show privilege [command]
```

*command* - Displays the privilege level for all commands modified by the *privilege* command.

**Command Mode**

Privileged Exec
Example
This example shows the privilege level for any command modified by the `privilege` command.

```
Console#show privilege command
privilege line all level 0 accounting
privilege exec level 15 ping
Console(config)#
```

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

**Table 36: Authentication Sequence Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication enable</td>
<td>Defines the authentication method and precedence for command mode change</td>
<td>GC</td>
</tr>
<tr>
<td>authentication login</td>
<td>Defines logon authentication method and precedence</td>
<td>GC</td>
</tr>
</tbody>
</table>

**authentication enable**

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the `enable` command. Use the `no` form to restore the default.

**Syntax**

```
authentication enable {[local] [radius] [tacacs]}

no authentication enable
```

**local** - Use local password only.

**radius** - Use RADIUS server password only.

**tacacs** - Use TACACS server password.

**Default Setting**
Local

**Command Mode**
Global Configuration

**Command Usage**
- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

◆ You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "authentication enable radius tacacs local," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```console
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

**enable password** - sets the password for changing command modes (204)

**authentication login**

This command defines the login authentication method and precedence. Use the *no* form to restore the default.

**Syntax**

```
authentication login {local [radius] [tacacs]}
no authentication login
```

**Default Setting**

Local

**Command Mode**

Global Configuration

**Command Usage**

◆ RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "authentication login radius tacacs local," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
```

Related Commands
username - for setting the local user names and passwords (205)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 37: RADIUS Client Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-server acct-port</td>
<td>Sets the RADIUS server network port</td>
<td>GC</td>
</tr>
<tr>
<td>radius-server auth-port</td>
<td>Sets the RADIUS server network port</td>
<td>GC</td>
</tr>
<tr>
<td>radius-server host</td>
<td>Specifies the RADIUS server</td>
<td>GC</td>
</tr>
<tr>
<td>radius-server key</td>
<td>Sets the RADIUS encryption key</td>
<td>GC</td>
</tr>
<tr>
<td>radius-server retransmit</td>
<td>Sets the number of retries</td>
<td>GC</td>
</tr>
<tr>
<td>radius-server timeout</td>
<td>Sets the interval between sending authentication requests</td>
<td>GC</td>
</tr>
<tr>
<td>show radius-server</td>
<td>Shows the current RADIUS settings</td>
<td>PE</td>
</tr>
</tbody>
</table>

radius-server acct-port

This command sets the RADIUS server network port for accounting messages. Use the no form to restore the default.

Syntax

```
radius-server acct-port port-number
no radius-server acct-port
```

`port-number` - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)
**radius-server auth-port**

This command sets the RADIUS server network port. Use the **no** form to restore the default.

**Syntax**

```
radius-server auth-port port-number
```

```
no radius-server auth-port
```

- **port-number** - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

**Default Setting**

1812

**Command Mode**

Global Configuration

**Example**

```
Console(config)#radius-server auth-port 181
Console(config)#
```

**radius-server host**

This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

**Syntax**

```
[no] radius-server index host host-ip-address [acct-port acct-port] [auth-port auth-port] [key key] [retransmit retransmit] [timeout timeout]
```

- **index** - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.
- **host-ip-address** - IP address of server.
- **acct-port** - RADIUS server UDP port used for accounting messages. (Range: 1-65535)
**auth-port** - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

**key** - Encryption key used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)

**retransmit** - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

**timeout** - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

### Default Setting

- **auth-port** - 1812
- **acct-port** - 1813
- **timeout** - 5 seconds
- **retransmit** - 2

### Command Mode

Global Configuration

### Example

```
Console(config)#radius-server 1 host 192.168.1.20 acct-port 181 timeout 10 retransmit 5 key green
Console(config)#
```

**radius-server key**  This command sets the RADIUS encryption key. Use the `no` form to restore the default.

### Syntax

```
radius-server key  key-string
```

```
no radius-server key
```

**key-string** - Encryption key used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Example

```
Console(config)#radius-server key green
Console(config)#
```
**radius-server retransmit**

This command sets the number of retries. Use the `no` form to restore the default.

**Syntax**

```
radius-server retransmit number-of-retries
```

```
no radius-server retransmit
```

- `number-of-retries` - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

**Default Setting**

2

**Command Mode**

Global Configuration

**Example**

```
Console(config)#radius-server retransmit 5
Console(config)#
```

---

**radius-server timeout**

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the `no` form to restore the default.

**Syntax**

```
radius-server timeout number-of-seconds
```

```
no radius-server timeout
```

- `number-of-seconds` - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

**Default Setting**

5

**Command Mode**

Global Configuration

**Example**

```
Console(config)#radius-server timeout 10
Console(config)#
```
**show radius-server**  
This command displays the current settings for the RADIUS server.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**

```console
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
  Authentication Port Number : 1812
  Accounting Port Number     : 1813
  Retransmit Times           : 2
  Request Timeout            : 5

Server 1:
  Server IP Address          : 192.168.1.1
  Authentication Port Number : 1812
  Accounting Port Number     : 1813
  Retransmit Times           : 2
  Request Timeout            : 5

Radius Server Group:
  Group Name                Member Index
    ------------------------- -------------
    radius                    1

Console#
```

---

**TACACS+ Client**

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

**Table 38: TACACS+ Client Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host</td>
<td>Specifies the TACACS+ server and optional parameters</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>Sets the TACACS+ encryption key</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server port</td>
<td>Specifies the TACACS+ server network port</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server retransmit</td>
<td>Sets the number of retries</td>
<td>GC</td>
</tr>
<tr>
<td>tacacs-server timeout</td>
<td>Sets the interval between sending authentication requests</td>
<td>GC</td>
</tr>
<tr>
<td>show tacacs-server</td>
<td>Shows the current TACACS+ settings</td>
<td>GC</td>
</tr>
</tbody>
</table>
**tacacs-server host**  This command specifies the TACACS+ server and other optional parameters. Use the no form to remove the server, or to restore the default values.

**Syntax**

```
tacacs-server index host host-ip-address [key key] [port port-number] [retransmit retransmit] [timeout timeout]
```

```
no tacacs-server index
```

- **index** - The index for this server. (Range: 1)
- **host-ip-address** - IP address of a TACACS+ server.
- **key** - Encryption key used to authenticate logon access for the client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)
- **port-number** - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)
- **retransmit** - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1-30)
- **timeout** - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

**Default Setting**

- authentication port - 49
- timeout - 5 seconds
- retransmit - 2

**Command Mode**

Global Configuration

**Example**

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10 retransmit 5 key green
Console(config)#
```

**tacacs-server key**  This command sets the TACACS+ encryption key. Use the no form to restore the default.

**Syntax**

```
tacacs-server key key-string
```

```
no tacacs-server key
```

- **key-string** - Encryption key used to authenticate logon access for the client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)
**Default Setting**  
None

**Command Mode**  
Global Configuration

**Example**
```
Console(config)#tacacs-server key green  
Console(config)#
```

**tacacs-server port**  
This command specifies the TACACS+ server network port. Use the no form to restore the default.

**Syntax**
```
tacacs-server port port-number  
no tacacs-server port  
port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)
```

**Default Setting**  
49

**Command Mode**  
Global Configuration

**Example**
```
Console(config)#tacacs-server port 181  
Console(config)#
```

**tacacs-server retransmit**  
This command sets the number of retries. Use the no form to restore the default.

**Syntax**
```
tacacs-server retransmit number-of-retries  
no tacacs-server retransmit  
number-of-retries - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1 - 30)
```

**Default Setting**  
2

**Command Mode**  
Global Configuration
**Example**

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

**tacacs-server timeout** This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the `no` form to restore the default.

**Syntax**

```
tacacs-server timeout number-of-seconds
```

```
no tacacs-server timeout
```

- `number-of-seconds` - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

**Default Setting**

5

**Command Mode**

Global Configuration

**Example**

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

**show tacacs-server** This command displays the current settings for the TACACS+ server.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```
Console#show tacacs-server
```

Remote TACACS+ Server Configuration:

Global Settings:
- Server Port Number : 49
- Retransmit Times : 2
- Timeout : 5

Server 1:
- Server IP Address : 192.168.1.25
- Server Port Number : 181
- Retransmit Times : 2
- Timeout : 4
The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

### Table 39: AAA Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting commands</td>
<td>Enables accounting of Exec mode commands</td>
<td>GC</td>
</tr>
<tr>
<td>aaa accounting dot1x</td>
<td>Enables accounting of 802.1X services</td>
<td>GC</td>
</tr>
<tr>
<td>aaa accounting exec</td>
<td>Enables accounting of Exec services</td>
<td>GC</td>
</tr>
<tr>
<td>aaa accounting update</td>
<td>Enables periodic updates to be sent to the accounting server</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authorization commands</td>
<td>Enables authorization of local console or Telnet sessions</td>
<td>GC</td>
</tr>
<tr>
<td>aaa authorization exec</td>
<td>Enables authorization of Exec sessions</td>
<td>GC</td>
</tr>
<tr>
<td>aaa group server</td>
<td>Groups security servers in to defined lists</td>
<td>GC</td>
</tr>
<tr>
<td>server</td>
<td>Configures the IP address of a server in a group list</td>
<td>SG</td>
</tr>
<tr>
<td>accounting dot1x</td>
<td>Applies an accounting method to an interface for 802.1X service requests</td>
<td>IC</td>
</tr>
<tr>
<td>accounting commands</td>
<td>Applies an accounting method to CLI commands entered by a user</td>
<td>Line</td>
</tr>
<tr>
<td>accounting exec</td>
<td>Applies an accounting method to local console, Telnet or SSH connections</td>
<td>Line</td>
</tr>
<tr>
<td>authorization commands</td>
<td>Applies an authorization method to local console or Telnet sessions</td>
<td>Line</td>
</tr>
<tr>
<td>authorization exec</td>
<td>Applies an authorization method to local console or Telnet sessions</td>
<td>Line</td>
</tr>
<tr>
<td>show accounting</td>
<td>Displays all accounting information</td>
<td>PE</td>
</tr>
</tbody>
</table>
This command enables the accounting of Exec mode commands. Use the no form to disable the accounting service.

Syntax

```
aaa accounting commands level {default | method-name} start-stop group
  {tacacs+ | server-group}
```

```
no aaa accounting commands level {default | method-name}
```

- `level` - The privilege level for executing commands. (Range: 0-15)
- `default` - Specifies the default accounting method for service requests.
- `method-name` - Specifies an accounting method for service requests. (Range: 1-64 characters)
- `start-stop` - Records accounting from starting point and stopping point.
- `group` - Specifies the server group to use.
  - `tacacs+` - Specifies all TACACS+ hosts configured with the tacacs-server host command.
  - `server-group` - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- The accounting of Exec mode commands is only supported by TACACS+ servers.

- Note that the default and method-name fields are only used to describe the accounting method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

Example

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
```

```
Console(config)#
```
aaa accounting dot1x  This command enables the accounting of requested 802.1X services for network access. Use the no form to disable the accounting service.

Syntax

    aaa accounting dot1x {default | method-name}
    start-stop group {radius | tacacs+ | server-group}

    no aaa accounting dot1x {default | method-name}

- default - Specifies the default accounting method for service requests.
- method-name - Specifies an accounting method for service requests. (Range: 1-255 characters)
- start-stop - Records accounting from starting point and stopping point.
- group - Specifies the server group to use.
  - radius - Specifies all RADIUS hosts configure with the radius-server host command.
  - tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.
  - server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

Default Setting
Accounting is not enabled
No servers are specified

Command Mode
Global Configuration

Command Usage
Note that the default and method-name fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

    Console(config)#aaa accounting dot1x default start-stop group radius
    Console(config)#

aaa accounting exec  This command enables the accounting of requested Exec services for network access. Use the no form to disable the accounting service.

Syntax

    aaa accounting exec {default | method-name}
    start-stop group {radius | tacacs+ | server-group}

    no aaa accounting exec {default | method-name}
default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-255 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radius-server
host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server
host command.

server-group - Specifies the name of a server group configured with the
aaa group server command. (Range: 1-64 characters)

Default Setting
Accounting is not enabled
No servers are specified

Command Mode
Global Configuration

Command Usage
◆ This command runs accounting for Exec service requests for the local console
and Telnet connections.

◆ Note that the default and method-name fields are only used to describe the
accounting method(s) configured on the specified RADIUS or TACACS+ servers,
and do not actually send any information to the servers about the methods to
use.

Example

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update - This command enables the sending of periodic updates to the accounting server.
Use the no form to restore the default setting.

Syntax

```
aaa accounting update [periodic interval]
```

no aaa accounting update

interval - Sends an interim accounting record to the server at this interval.
(Range: 0-2147483647 minutes; where 0 means disabled)

Default Setting
1 minute
AAA

Chapter 7  Authentication Commands

Command Mode
Global Configuration

Command Usage
◆ When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.

◆ Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

Example

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization commands
This command enables the authorization for CLI commands entered via a local console or Telnet connection. Use the no form to disable the authorization service.

Syntax

```
aaa authorization commands level {default | method-name} group {tacacs+ | server-group}
```

- `level` - The privilege level for executing commands. (Range: 0-15)
- `default` - Specifies the default authorization method for CLI access.
- `method-name` - Specifies an authorization method for CLI access. (Range: 1-64 characters)
- `group` - Specifies the server group to use.
  - `tacacs+` - Specifies all TACACS+ hosts configured with the tacacs-server host command.
  - `server-group` - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

Default Setting
Authorization is not enabled
No servers are specified

Command Mode
Global Configuration

Command Usage
◆ This command performs authorization to determine if a user is allowed to submit CLI commands at the specified privilege level.

◆ AAA authentication must be enabled before authorization is enabled.
If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

Example

```
Console(config)#aaa authorization commands 0 default group tacacs+
Console(config)#
```

aaa authorization exec

This command enables the authorization for Exec access. Use the no form to disable the authorization service.

Syntax

```
aaa authorization exec {default | method-name}
  group {tacacs+ | server-group}

no aaa authorization exec {default | method-name}
  default - Specifies the default authorization method for Exec access.
  method-name - Specifies an authorization method for Exec access.
  (Range: 1-64 characters)
  group - Specifies the server group to use.
  tacacs+ - Specifies all TACACS+ hosts configured with the tacacs-server host command.
  server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)
```

Default Setting
Authorization is not enabled
No servers are specified

Command Mode
Global Configuration

Command Usage
● This command performs authorization to determine if a user is allowed to run an Exec shell.

● AAA authentication must be enabled before authorization is enabled.

● If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.
Example

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

**aaa group server** Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the no form of this command.

**Syntax**

```
[no] aaa group server (radius | tacacs+) group-name
```

- **radius** - Defines a RADIUS server group.
- **tacacs+** - Defines a TACACS+ server group.
- **group-name** - A text string that names a security server group. (Range: 1-255 characters)

**Default Setting**
None

**Command Mode**
Global Configuration

**Example**

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

**server** This command adds a security server to an AAA server group. Use the no form to remove the associated server from the group.

**Syntax**

```
[no] server (index | ip-address)
```

- **index** - Specifies the server index. (Range: RADIUS 1-5, TACACS+ 1)
- **ip-address** - Specifies the host IP address of a server.

**Default Setting**
None

**Command Mode**
Server Group Configuration

**Command Usage**
- When specifying the index for a RADIUS server, that server index must already be defined by the radius-server host command.
When specifying the index for a TACACS+ server, that server index must already be defined by the `tacacs-server host` command.

**Example**

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

**accounting dot1x** This command applies an accounting method for 802.1X service requests on an interface. Use the `no` form to disable accounting on the interface.

**Syntax**

```
accounting dot1x {default | list-name}
no accounting dot1x
```

- `default` - Specifies the default method list created with the `aaa accounting dot1x` command.
- `list-name` - Specifies a method list created with the `aaa accounting dot1x` command.

**Default Setting**

None

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

**accounting commands** This command applies an accounting method to entered CLI commands. Use the `no` form to disable accounting for entered CLI commands.

**Syntax**

```
accounting commands level {default | list-name}
no accounting commands level
```

- `level` - The privilege level for executing commands. (Range: 0-15)
- `default` - Specifies the default method list created with the `aaa accounting commands` command.
- `list-name` - Specifies a method list created with the `aaa accounting commands` command.
**Default Setting**
None

**Command Mode**
Line Configuration

**Example**
```
Console(config)#line console
Console(config-line)#accounting commands 15 default
Console(config-line)#
```

**accounting exec**
This command applies an accounting method to local console, Telnet or SSH connections. Use the no form to disable accounting on the line.

**Syntax**
```
accounting exec (default | list-name)
```

**no accounting exec**
- default - Specifies the default method list created with the aaa accounting exec command.
- list-name - Specifies a method list created with the aaa accounting exec command.

**Default Setting**
None

**Command Mode**
Line Configuration

**Example**
```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```
**authorization commands**

This command applies an authorization method to local console, Telnet or SSH connections at a specified privilege level. Use the `no` form to disable authorization on the line.

**Syntax**

```
authorization commands level {default | list-name}
no authorization commands level
```

- `level` - The privilege level for executing commands. (Range: 0-15)
- `default` - Specifies the default method list created with the `aaa authorization exec` command.
- `list-name` - Specifies a method list created with the `aaa authorization exec` command.

**Default Setting**

None

**Command Mode**

Line Configuration

**Example**

```
Console(config)#line console
Console(config-line)#authorization commands tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization commands default
Console(config-line)#
```

**authorization exec**

This command applies an authorization method to local console, Telnet or SSH connections. Use the `no` form to disable authorization on the line.

**Syntax**

```
authorization exec {default | list-name}
no authorization exec
```

- `default` - Specifies the default method list created with the `aaa authorization exec` command.
- `list-name` - Specifies a method list created with the `aaa authorization exec` command.

**Default Setting**

None

**Command Mode**

Line Configuration
Example

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

**show accounting**  This command displays the current accounting settings per function and per port.

**Syntax**

```
show accounting [commands [level]] | [[dot1x [statistics [username user-name | interface interface]] | exec [statistics] | statistics]
commands  - Displays command accounting information.
level  - Displays command accounting information for a specifiable command level.
dot1x  - Displays dot1x accounting information.
exec  - Displays Exec accounting records.
statistics  - Displays accounting records.
user-name  - Displays accounting records for a specifiable username.
interface

ethernet unit/port
  unit  - Unit identifier. (Range: 1)
  port  - Port number. (Range: 1-28/52)
```

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```
Console#show accounting
Accounting Type: dot1x
  Method List  : default
  Group List   : radius
  Interface    : Eth 1/1
  Method List  : tps
  Group List   : radius
  Interface    : Eth 1/2
Accounting Type: EXEC
  Method List  : default
  Group List   : tacacs+
```
Web Server

This section describes commands used to configure web browser management access to the switch.

Table 40: Web Server Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip http port</td>
<td>Specifies the port to be used by the web browser interface</td>
<td>GC</td>
</tr>
<tr>
<td>ip http server</td>
<td>Allows the switch to be monitored or configured from a browser</td>
<td>GC</td>
</tr>
<tr>
<td>ip http secure-port</td>
<td>Specifies the UDP port number for HTTPS</td>
<td>GC</td>
</tr>
<tr>
<td>ip http secure-server</td>
<td>Enables HTTPS (HTTP/SSL) for encrypted communications</td>
<td>GC</td>
</tr>
</tbody>
</table>

**ip http port**  This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

**Syntax**

```
ip http port port-number
no ip http port
```

*port-number* - The TCP port to be used by the browser interface. (Range: 1-65535)

**Default Setting**

80

**Command Mode**

Global Configuration

**Example**

```
Console(config)#ip http port 769
Console(config)#
```

**Related Commands**

ip http server (230)
show system (103)
**ip http server**  This command allows this device to be monitored or configured from a browser. Use the no form to disable this function.

**Syntax**

```
[no] ip http server
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Example**

```
Console(config)#ip http server
```

**Related Commands**

ip http port (229)
show system (103)

---

**ip http secure-port**  This command specifies the TCP port number used for HTTPS connection to the switch's web interface. Use the no form to restore the default port.

**Syntax**

```
ip http secure-port port_number
```

```
no ip http secure-port
```

- `port_number` – The TCP port used for HTTPS. (Range: 1-65535)

**Default Setting**

443

**Command Mode**

Global Configuration

**Command Usage**

- You cannot configure the HTTP and HTTPS servers to use the same port.

- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: `https://device:port_number`

**Example**

```
Console(config)#ip http secure-port 1000
```

---

---
Related Commands
ip http secure-server (231)
show system (103)

**ip http secure-server**  This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

**Syntax**

```plaintext
[no] ip http secure-server
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Command Usage**

◆ Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.

◆ If you enable HTTPS, you must indicate this in the URL that you specify in your browser: `https://device[:port_number]`

◆ When you start HTTPS, the connection is established in this way:

  - The client authenticates the server using the server’s digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.

◆ The client and server establish a secure encrypted connection.

A padlock icon should appear in the status bar for Internet Explorer 6, Mozilla Firefox 30, or Google Chrome 29, or more recent versions.

The following web browsers and operating systems currently support HTTPS:

Table 41: HTTPS System Support

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 6.x or later</td>
<td>Windows 98, Windows NT (with service pack 6a), Windows 2000, XP, Vista, 7, 8</td>
</tr>
</tbody>
</table>
Table 41: HTTPS System Support (Continued)

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox 30 or later</td>
<td>Windows 2000, XP, Vista, 7, 8, Linux</td>
</tr>
<tr>
<td>Google Chrome 29 or later</td>
<td>Windows XP, Vista, 7, 8</td>
</tr>
</tbody>
</table>

- To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” in the System Reference Guide. Also refer to the `copy tftp https-certificate` command.

- Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands
- `ip http secure-port (230)`
- `copy tftp https-certificate (110)`
- `show system (103)`

Telnet Server

This section describes commands used to configure Telnet management access to the switch.

Table 42: Telnet Server Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip telnet max-sessions</td>
<td>Specifies the maximum number of Telnet sessions that can simultaneously connect to this system</td>
<td>GC</td>
</tr>
<tr>
<td>ip telnet port</td>
<td>Specifies the port to be used by the Telnet interface</td>
<td>GC</td>
</tr>
<tr>
<td>ip telnet server</td>
<td>Allows the switch to be monitored or configured from Telnet</td>
<td>GC</td>
</tr>
<tr>
<td>show ip telnet</td>
<td>Displays configuration settings for the Telnet server</td>
<td>PE</td>
</tr>
</tbody>
</table>

Note: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the `telnet` command at the Privileged Exec configuration level.
**ip telnet max-sessions**  This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** form to restore the default setting.

**Syntax**

```
ip telnet max-sessions session-count
no ip telnet max-sessions
```

*session-count* - The maximum number of allowed Telnet session.
(Range: 0-8)

**Default Setting**

8 sessions

**Command Mode**

Global Configuration

**Command Usage**

A maximum of four sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number or four sessions).

**Example**

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

**ip telnet port**  This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

**Syntax**

```
ip telnet port port-number
no telnet port
```

*port-number* - The TCP port number to be used by the browser interface.
(Range: 1-65535)

**Default Setting**

23

**Command Mode**

Global Configuration

**Example**

```
Console(config)#ip telnet port 123
Console(config)#
```
**ip telnet server**  This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

**Syntax**
```
[no] ip telnet server
```

**Default Setting**
Enabled

**Command Mode**
Global Configuration

**Example**
```
Console(config)#ip telnet server
Console(config)#
```

**show ip telnet**  This command displays the configuration settings for the Telnet server.

**Command Mode**
Normal Exec, Privileged Exec

**Example**
```
Console#show ip telnet
IP Telnet Configuration:

   Telnet Status: Enabled
   Telnet Service Port: 23
   Telnet Max Session: 8

Console#
```

---

**Secure Shell**

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

**Note:** The switch supports both SSH Version 1.5 and 2.0 clients.
The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the `authentication login` command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the `ip ssh crypto host-key generate` command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:
3. Import Client’s Public Key to the Switch – Use the `copy tftp public-key` command to copy a file containing the public key for all the SSH client’s granted management access to the switch. (Note that these clients must be configured locally on the switch with the `username` command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

```
1024 35
1341081685609893210409449201554253476316419218729589211437388005553616163105
1775940838663110929213222628519254374603100937187721199696317813662774141689
8513204917204830392543241016379975923714490119380060902539484084827178194372
2884025331159521348610229029789827213353267131629432532818915045306393916643
steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the `ip ssh server` command to enable the SSH server on the switch.

6. Authentication – One of the following authentication methods is employed:

   **Password Authentication (for SSH v1.5 or V2 Clients)**
   - The client sends its password to the server.
   - The switch compares the client’s password to those stored in memory.
   - If a match is found, the connection is allowed.

   **Public Key Authentication** – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

   **Authenticating SSH v1.5 Clients**
   - The client sends its RSA public key to the switch.
   - The switch compares the client’s public key to those stored in memory.
c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user’s public key, and sends it to the client.

d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.

e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client’s private key corresponds to an authorized public key, and the client is authenticated.

**Authenticating SSH v2 Clients**

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.

b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

c. The client sends a signature generated using the private key to the switch.

d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

---

**Note:** The SSH server supports up to eight client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

**Note:** The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

---

**ip ssh authentication-retries**

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the `no` form to restore the default setting.

**Syntax**

```
ip ssh authentication-retries count
no ip ssh authentication-retries
```

- `count` – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

**Default Setting**

3

**Command Mode**

Global Configuration
Example

```console
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

Related Commands

show ip ssh (242)

**ip ssh server**

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

**Syntax**

```console
[no] ip ssh server
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

◆ The SSH server supports up to eight client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

◆ The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

◆ You must generate DSA and RSA host keys before enabling the SSH server.

Example

```console
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (240)
show ssh (244)
**ip ssh server-key size**  This command sets the SSH server key size. Use the **no** form to restore the default setting.

**Syntax**

```
  ip ssh server-key size key-size
  no ip ssh server-key size
```

  *key-size* – The size of server key. (Range: 512-1024 bits)

**Default Setting**

768 bits

**Command Mode**

Global Configuration

**Command Usage**

The server key is a private key that is never shared outside the switch. The host key is shared with the SSH client, and is fixed at 1024 bits.

**Example**

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

**ip ssh timeout**  This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

**Syntax**

```
  ip ssh timeout seconds
  no ip ssh timeout
```

  *seconds* – The timeout for client response during SSH negotiation.

  (Range: 1-120)

**Default Setting**

120 seconds

**Command Mode**

Global Configuration

**Command Usage**

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.
Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands
exec-timeout (122)
show ip ssh (242)

delete public-key This command deletes the specified user’s public key.

Syntax

```
delete public-key username [dsa | rsa]
```

- **username** – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting
Deletes both the DSA and RSA key.

Command Mode
Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate This command generates the host key pair (i.e., public and private).

Syntax

```
ip ssh crypto host-key generate [dsa | rsa]
```

- **dsa** – DSA (Version 2) key type.
- **rsa** – RSA (Version 1) key type.

Default Setting
Generates both the DSA and RSA key pairs.

Command Mode
Privileged Exec
**Command Usage**

- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- This command stores the host key pair in memory (i.e., RAM). Use the `ip ssh save host-key` command to save the host key pair to flash memory.

- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.

- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

**Example**

```plaintext
Console#ip ssh crypto host-key generate dsa
Console# 
```

**Related Commands**

- `ip ssh crypto zeroize (241)`
- `ip ssh save host-key (242)`

**ip ssh crypto zeroize**  This command clears the host key from memory (i.e. RAM).

**Syntax**

```plaintext
ip ssh crypto zeroize [dsa | rsa]
```

- `dsa` – DSA key type.
- `rsa` – RSA key type.

**Default Setting**

Clears both the DSA and RSA key.

**Command Mode**

Privileged Exec

**Command Usage**

- This command clears the host key from volatile memory (RAM). Use the `no ip ssh save host-key` command to clear the host key from flash memory.

- The SSH server must be disabled before you can execute this command.

**Example**

```plaintext
Console#ip ssh crypto zeroize dsa
Console# 
```
Related Commands
ip ssh crypto host-key generate (240)
ip ssh save host-key (242)
no ip ssh server (238)

**ip ssh save host-key** This command saves the host key from RAM to flash memory.

**Syntax**

```
ip ssh save host-key
```

**Default Setting**
Saves both the DSA and RSA key.

**Command Mode**
Privileged Exec

**Example**

```
Console#ip ssh save host-key
Console#
```

**Related Commands**

**show ip ssh** This command displays the connection settings used when authenticating client access to the SSH server.

**Command Mode**
Privileged Exec

**Example**

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size : 768 bits
Console#
```
show public-key  This command shows the public key for the specified user or for the host.

**Syntax**

```
show public-key [user [username] host]
```

*username* – Name of an SSH user. (Range: 1-32 characters)

**Default Setting**

Shows all public keys.

**Command Mode**

Privileged Exec

**Command Usage**

◆ If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.

◆ When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

**Example**

```
Console#show public-key host
Host: 
RSA: 
1024  65537  132369406582547640313827955256536375972835523527972629521130241
07194210615557942459093923609695405036277525755625100386613089893983452310
32328021498866192159556685988799891919505883940181374406489087917951603587768
185490002381313416250083847818449522087429212255691665655296328163516964040831
5547660664151657116381

Console#
```
show ssh  This command displays the current SSH server connections.

**Command Mode**
Privileged Exec

**Example**

```
Console#show ssh
Connection  Version  State          Username  Encryption
           1          2.0  Session-Started admin  ctos aes128-cbc-hmac-md5
stoc aes128-cbc-hmac-md5
Console#
```

**Table 44: show ssh - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>The session number. (Range: 1-8)</td>
</tr>
<tr>
<td>Version</td>
<td>The Secure Shell version number.</td>
</tr>
<tr>
<td>State</td>
<td>The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)</td>
</tr>
<tr>
<td>Username</td>
<td>The user name of the client.</td>
</tr>
</tbody>
</table>

**802.1X Port Authentication**

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

**Table 45: 802.1X Port Authentication Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dot1x default</td>
<td>Resets all dot1x parameters to their default values</td>
<td>GC</td>
</tr>
<tr>
<td>dot1x eapol-pass-through</td>
<td>Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled</td>
<td>GC</td>
</tr>
<tr>
<td>dot1x system-auth-control</td>
<td>Enables dot1x globally on the switch.</td>
<td>GC</td>
</tr>
<tr>
<td><strong>Authenticator Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dot1x intrusion-action</td>
<td>Sets the port response to intrusion when authentication fails</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x max-reauth-req</td>
<td>Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process</td>
<td>IC</td>
</tr>
<tr>
<td>dot1x max-req</td>
<td>Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session</td>
<td>IC</td>
</tr>
</tbody>
</table>
Table 45: 802.1X Port Authentication Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x operation-mode</code></td>
<td>Allows single or multiple hosts on an dot1x port</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x port-control</code></td>
<td>Sets dot1x mode for a port interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x re-authentication</code></td>
<td>Enables re-authentication for all ports</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x timeout quiet-period</code></td>
<td>Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x timeout re-authperiod</code></td>
<td>Sets the time period after which a connected client must be re-authenticated</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x timeout supp-timeout</code></td>
<td>Sets the interval for a supplicant to respond</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x timeout tx-period</code></td>
<td>Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet</td>
<td>IC</td>
</tr>
<tr>
<td><code>dot1x re-authenticate</code></td>
<td>Forces re-authentication on specific ports</td>
<td>PE</td>
</tr>
</tbody>
</table>

### Supplicant Commands

- `dot1x identity profile` Configures dot1x supplicant user name and password
- `dot1x max-start` Sets the maximum number of times that a port supplicant will send an EAP start frame to the client
- `dot1x pae supplicant` Enables dot1x supplicant mode on an interface
- `dot1x timeout auth-period` Sets the time that a supplicant port waits for a response from the authenticator
- `dot1x timeout held-period` Sets the time a port waits after the maximum start count has been exceeded before attempting to find another authenticator
- `dot1x timeout start-period` Sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator

### Information Display Commands

- `show dot1x` Shows all dot1x related information

### General Commands

#### `dot1x default`

This command sets all configurable dot1x authenticator global and port settings to their default values.

**Command Mode**

Global Configuration

**Command Usage**

This command resets the following commands to their default settings:

- `dot1x system-auth-control`
- `dot1x eapol-pass-through`
- `dot1x port-control`
- `dot1x port-control multi-host max-count`
Chapter 7 | Authentication Commands
802.1X Port Authentication

- dot1x operation-mode
- dot1x max-req
- dot1x timeout quiet-period
- dot1x timeout tx-period
- dot1x timeout re-authperiod
- dot1x timeout sup-timeout
- dot1x re-authentication
- dot1x intrusion-action

Example

```
Console(config)#dot1x default
Console(config)#
```

**Example**

This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the **no** form to restore the default.

**Syntax**

```
[no] dot1x eapol-pass-through
```

**Default Setting**
Discards all EAPOL frames when dot1x is globally disabled

**Command Mode**
Global Configuration

**Command Usage**
- When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the **dot1x eapol pass-through** command can be used to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

- When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the **no dot1x eapol-pass-through** command can be used to discard unnecessary EAPOL traffic.

**Example**

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```
**dot1x system-auth-control**  This command enables IEEE 802.1X port authentication globally on the switch. Use the `no` form to restore the default.

**Syntax**

```
[no] dot1x system-auth-control
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Example**

```
Console(config)#dot1x system-auth-control
Console(config)#
```

---

**Authenticator Commands**

**dot1x intrusion-action**  This command sets the port’s response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the `no` form to reset the default.

**Syntax**

```
dot1x intrusion-action {block-traffic | guest-vlan}
no dot1x intrusion-action
```

- `block-traffic` - Blocks traffic on this port.
- `guest-vlan` - Assigns the user to the Guest VLAN.

**Default**

block-traffic

**Command Mode**

Interface Configuration

**Command Usage**

For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the `vlan database` command) and assigned as the guest VLAN for the port (see the `network-access guest-vlan` command).

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```
**dot1x max-reauth-req**  This command sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. Use the no form to restore the default.

**Syntax**

```
dot1x max-reauth-req count
no dot1x max-reauth-req
```

`count` – The maximum number of requests (Range: 1-10)

**Default**

2

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-reauth-req 2
Console(config-if)#
```

**dot1x max-req**  This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the no form to restore the default.

**Syntax**

```
dot1x max-req count
no dot1x max-req
```

`count` – The maximum number of requests (Range: 1-10)

**Default**

2

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```
**dot1x operation-mode**  This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the no form with no keywords to restore the default to single host. Use the no form with the **multi-host max-count** keywords to restore the default maximum count.

**Syntax**

```
dot1x operation-mode {single-host | multi-host [max-count count] | mac-based-auth}
```

```
no dot1x operation-mode [multi-host max-count]
```

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple hosts to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
- **count** – The maximum number of hosts that can connect to a port.
  (Range: 1-1024; Default: 5)
- **mac-based** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

**Default**

Single-host

**Command Mode**

Interface Configuration

**Command Usage**

- The “max-count” parameter specified by this command is only effective if the dot1x mode is set to “auto” by the **dot1x port-control** command.
- In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- In “mac-based-auth” mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```
**dot1x port-control**  This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

**Syntax**

```
dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control
```

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

**Default**

force-authorized

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

**dot1x re-authentication**  This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

**Syntax**

```
[no] dot1x re-authentication
```

**Command Mode**

Interface Configuration

**Command Usage**

- The re-authentication process verifies the connected client’s user ID and password on the RADIUS server. During re-authentication, the client remains connected to the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

- The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.
Example

```console
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

Related Commands
dot1x timeout re-authperiod (251)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count (see page 248) has been exceeded before attempting to acquire a new client. Use the no form to reset the default.

**Syntax**

```
dot1x timeout quiet-period seconds
no dot1x timeout quiet-period
```

*seconds* - The number of seconds. (Range: 1-65535)

**Default**

60 seconds

**Command Mode**

Interface Configuration

**Example**

```console
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the no form of this command to reset the default.

**Syntax**

```
dot1x timeout re-authperiod seconds
no dot1x timeout re-authperiod
```

*seconds* - The number of seconds. (Range: 1-65535)

**Default**

3600 seconds

**Command Mode**

Interface Configuration
Example

```console
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

**`dot1x timeout supp-timeout`**

This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

**Syntax**

```console
dot1x timeout supp-timeout seconds
no dot1x timeout supp-timeout
```

- `seconds` - The number of seconds. (Range: 1-65535)

**Default**

30 seconds

**Command Mode**

Interface Configuration

**Command Usage**

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

Example

```console
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

**`dot1x timeout tx-period`**

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

**Syntax**

```console
dot1x timeout tx-period seconds
no dot1x timeout tx-period
```

- `seconds` - The number of seconds. (Range: 1-65535)
Default
30 seconds

Command Mode
Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

```
dot1x re-authenticate [interface]
```

- **interface**
  - **ethernet unit/port**
    - *unit* - Unit identifier. (Range: 1)
    - *port* - Port number. (Range: 1-28/52)

Command Mode

Privileged Exec

Command Usage

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

Example

```
Console#dot1x re-authenticate
Console#
```
Supplicant Commands

**dot1x identity profile**  This command sets the dot1x supplicant user name and password. Use the **no** form to delete the identity settings.

**Syntax**

```
dot1x identity profile {username username | password password}
```

```
no dot1x identity profile {username | password}
```

*username* - Specifies the supplicant user name. (Range: 1-8 characters)

*password* - Specifies the supplicant password. (Range: 1-32 characters)

**Default**

No user name or password

**Command Mode**

Global Configuration

**Command Usage**

The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see the **dot1x pae supplicant** command).

**Example**

```
Console(config)#dot1x identity profile username steve
Console(config)#dot1x identity profile password excess
Console(config)#
```

**dot1x max-start**  This command sets the maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. Use the **no** form to restore the default value.

**Syntax**

```
dot1x max-start count
```

```
no dot1x max-start
```

*count* - Specifies the maximum number of EAP start frames.

(Range: 1-65535)

**Default**

3

**Command Mode**

Interface Configuration
**Example**

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x max-start 10
Console(config-if)#
```

**dot1x pae supplicant**  
This command enables dot1x supplicant mode on a port. Use the **no** form to disable dot1x supplicant mode on a port.

**Syntax**

```
[no] dot1x pae supplicant
```

**Default**  
Disabled

**Command Mode**  
Interface Configuration

**Command Usage**

- When devices attached to a port must submit requests to another authenticator on the network, configure the identity profile parameters (see **dot1x identity profile** command) which identify this switch as a supplicant, and enable dot1x supplicant mode for those ports which must authenticate clients through a remote authenticator using this command. In this mode the port will not respond to dot1x messages meant for an authenticator.

- This switch can be configured to serve as the authenticator on selected ports by setting the control mode to “auto” (see the **dot1x port-control** command), and as a supplicant on other ports by the setting the control mode to “force-authorized” and enabling dot1x supplicant mode with this command.

- A port cannot be configured as a dot1x supplicant if it is a member of a trunk or LACP is enabled on the port.

**Example**

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x pae supplicant
Console(config-if)#
```
**dot1x timeout auth-period** This command sets the time that a supplicant port waits for a response from the authenticator. Use the no form to restore the default setting.

**Syntax**

```
dot1x timeout auth-period seconds
no dot1x timeout auth-period
```

seconds - The number of seconds. (Range: 1-65535)

**Default**

30 seconds

**Command Mode**

Interface Configuration

**Command Usage**

This command sets the time that the supplicant waits for a response from the authenticator for packets other than EAPOL-Start.

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout auth-period 60
Console(config-if)#
```

**dot1x timeout held-period** This command sets the time that a supplicant port waits before resending its credentials to find a new authenticator. Use the no form to reset the default.

**Syntax**

```
dot1x timeout held-period seconds
no dot1x timeout held-period
```

seconds - The number of seconds. (Range: 1-65535)

**Default**

60 seconds

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout held-period 120
Console(config-if)#
```
**dot1x timeout start-period**  This command sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator. Use the no form to restore the default setting.

**Syntax**

```
dot1x timeout start-period seconds
no dot1x timeout start-period
```

- **seconds** - The number of seconds. (Range: 1-65535)

**Default**

30 seconds

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout start-period 60
Console(config-if)#
```

---

**Information Display Commands**

**show dot1x**  This command shows general port authentication related settings on the switch or a specific interface.

**Syntax**

```
show dot1x [statistics] [interface interface]

statistics - Displays dot1x status for each port.

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)
```

**Command Mode**

Privileged Exec

**Command Usage**

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch (page 247).
◆ **Authenticator Parameters** – Shows whether or not EAPOL pass-through is enabled (page 246).

◆ **Supplicant Parameters** – Shows the supplicant user name used when the switch responds to an MD5 challenge from an authenticator (page 254).

◆ **802.1X Port Summary** – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
  - Type – Administrative state for port access control (Enabled, Authenticator, or Supplicant).
  - Operation Mode– Allows single or multiple hosts (page 249).
  - Control Mode – Dot1x port control mode (page 250).
  - Authorized– Authorization status (yes or n/a - not authorized).

◆ **802.1X Port Details** – Displays the port access control parameters for each interface, including the following items:
  - Reauthentication – Periodic re-authentication (page 250).
  - Reauth Period – Time after which a connected client must be re-authenticated (page 251).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 251).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet (page 252).
  - Supplicant Timeout – Supplicant timeout.
  - Server Timeout – Server timeout. A RADIUS server must be set before the correct operational value of 10 seconds will be displayed in this field.
  - Reauth Max Retries – Maximum number of reauthentication attempts.
  - Max Request – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 248).
  - Operation Mode– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
  - Port Control– Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 250).
  - Intrusion Action– Shows the port response to intrusion when authentication fails (page 247).
  - Supplicant– MAC address of authorized client.

◆ **Authenticator PAE State Machine**
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, forceAuthorized, forceUnauthorized).
  - Reauth Count– Number of times connecting state is re-entered.
  - Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.
◆ **Backend State Machine**

- **State** – Current state (including request, response, success, fail, timeout, idle, initialize).
- **Request Count** – Number of EAP Request packets sent to the Supplicant without receiving a response.
- **Identifier (Server)** – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

◆ **Reauthentication State Machine**

State – Current state (including initialize, reauthenticate).

**Example**

```plaintext
Console#show dot1x
Global 802.1X Parameters
System Auth Control     : Enabled
Authenticator Parameters:
EAPOL Pass Through      : Disabled
Supplicant Parameters:
Identity Profile Username : steve

802.1X Port Summary

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Operation Mode</th>
<th>Control Mode</th>
<th>Authorized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>Disabled</td>
<td>Single-Host</td>
<td>Force-Authorized</td>
<td>Yes</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>Disabled</td>
<td>Single-Host</td>
<td>Force-Authorized</td>
<td>Yes</td>
</tr>
<tr>
<td>Eth 1/27</td>
<td>Disabled</td>
<td>Single-Host</td>
<td>Force-Authorized</td>
<td>Yes</td>
</tr>
<tr>
<td>Eth 1/28</td>
<td>Enabled</td>
<td>Single-Host</td>
<td>Auto</td>
<td>Yes</td>
</tr>
</tbody>
</table>

console#show dot1x interface ethernet 1/28
802.1X Authenticator is enabled on port 28
Reauthentication    : Enabled
Reauth Period       : 3600
Quiet Period        : 60
TX Period           : 30
Supplicant Timeout  : 30
Server Timeout      : 10
Reauth Max Retries  : 2
Max Request         : 2
Operation Mode      : Multi-host
Port Control        : Auto
Intrusion Action    : Block traffic
Supplicant          : 00-e0-29-94-34-65

Authenticator PAE State Machine
State               : Authenticated
Reauth Count        : 0
Current Identifier  : 3
```
Management IP Filter

This section describes commands used to configure IP management access to the switch.

Table 46: Management IP Filter Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>management</td>
<td>Configures IP addresses that are allowed management access</td>
<td>GC</td>
</tr>
<tr>
<td>show management</td>
<td>Displays the switch to be monitored or configured from a browser</td>
<td>PE</td>
</tr>
</tbody>
</table>

management This command specifies the client IP addresses that are allowed management access to the switch through various protocols. A list of up to 15 IP addresses or IP address groups can be specified. Use the no form to restore the default setting.

Syntax

```
[no] management [all-client | http-client | snmp-client | telnet-client]
start-address [end-address]
```

- all-client - Adds IP address(es) to all groups.
- http-client - Adds IP address(es) to the web group.
- snmp-client - Adds IP address(es) to the SNMP group.
- telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

default-address - The end address of a range.

Default Setting
All addresses

Command Mode
Global Configuration
Command Usage

◆ The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.

◆ If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.

◆ IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.

◆ When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.

◆ You cannot delete an individual address from a specified range. You must delete the entire range, and re-enter the addresses.

◆ You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example
This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

**show management**
This command displays the client IP addresses that are allowed management access to the switch through various protocols.

**Syntax**
```
show management {all-client | http-client | snmp-client | telnet-client}
```

- **all-client** - Displays IP addresses for all groups.
- **http-client** - Displays IP addresses for the web group.
- **snmp-client** - Displays IP addresses for the SNMP group.
- **telnet-client** - Displays IP addresses for the Telnet group.

**Command Mode**
Privileged Exec
Example

```console
Console#show management all-client
Management Ip Filter
HTTP-Client:
  Start IP address      End IP address
  -----------------------------------------------
  1. 192.168.1.19       192.168.1.19
  2. 192.168.1.25       192.168.1.30

SNMP-Client:
  Start IP address      End IP address
  -----------------------------------------------
  1. 192.168.1.19       192.168.1.19
  2. 192.168.1.25       192.168.1.30

TELNET-Client:
  Start IP address      End IP address
  -----------------------------------------------
  1. 192.168.1.19       192.168.1.19
  2. 192.168.1.25       192.168.1.30

Console#
```

**PPPoE Intermediate Agent**

This section describes commands used to configure the PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

**Table 47: PPPoE Intermediate Agent Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Enables the PPPoE IA globally on the switch</td>
<td>GC</td>
</tr>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Sets the access node identifier and generic error message for the switch</td>
<td>GC</td>
</tr>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Enables the PPPoE IA on an interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Sets the circuit-id or remote-id for an interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Sets the remote-id delimiter for an interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Sets the trust mode for an interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>pppoe intermediate-agent</code></td>
<td>Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server</td>
<td>IC</td>
</tr>
<tr>
<td><code>clear pppoe intermediate-agent statistics</code></td>
<td>Clears PPPoE IA statistics</td>
<td>PE</td>
</tr>
<tr>
<td><code>show pppoe intermediate-agent info</code></td>
<td>Displays PPPoE IA configuration settings</td>
<td>PE</td>
</tr>
<tr>
<td><code>show pppoe intermediate-agent statistics</code></td>
<td>Displays PPPoE IA statistics</td>
<td>PE</td>
</tr>
</tbody>
</table>
**pppoe intermediate-agent** This command enables the PPPoE Intermediate Agent globally on the switch. Use the **no** form to disable this feature.

**Syntax**

```
[no] pppoe intermediate-agent
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

◆ The switch inserts a tag identifying itself as a PPPoE Intermediate Agent residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports designated by the **pppoe intermediate-agent trust** command. The BRAS detects the presence of the subscriber's circuit-ID tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-ID attribute in PPP authentication and AAA accounting requests to a RADIUS server.

◆ PPPoE IA must be enabled globally by this command before this feature can be enabled on an interface using the **pppoe intermediate-agent port-enable** command.

**Example**

```
Console(config)# pppoe intermediate-agent
Console(config)#
```

**pppoe intermediate-agent format-type** This command sets the access node identifier and generic error message for the switch. Use the **no** form to restore the default settings.

**Syntax**

```
pppoe intermediate-agent format-type {access-node-identifier id-string | generic-error-message error-message}
no pppoe intermediate-agent format-type {access-node-identifier | generic-error-message}
```

- **id-string** - String identifying this switch as a PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters)

- **error-message** - An error message notifying the sender that the PPPoE Discovery packet was too large.
Default Setting
◆ Access Node Identifier: IP address of the first IPv4 interface on the switch.
◆ Generic Error Message: PPPoE Discover packet too large to process. Try reducing the number of tags added.

Command Mode
Global Configuration

Command Usage
◆ The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets.
◆ These messages are forwarded to all trusted ports designated by the pppoe intermediate-agent trust command.

Example
```
Console(config)#pppoe intermediate-agent format-type access-node-identifier billibong
Console(config)#
```

pppoe intermediate-agent port-enable
This command enables the PPPoE IA on an interface. Use the `no` form to disable this feature.

Syntax
```
[no] pppoe intermediate-agent port-enable
```

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
PPPoE IA must also be enabled globally on the switch for this command to take effect.

Example
```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-enable
Console(config-if)#
```
This command sets the circuit-id or remote-id for an interface. Use the `no` form to restore the default settings.

**Syntax**

```
pppoe intermediate-agent port-format-type {circuit-id | remote-id} [id-string]
```

- `circuit-id` - String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters)
- `remote-id` - String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters)

**Default Setting**

- `circuit-id`: unit/port:vlan-id or 0/trunk-id:vlan-id
- `remote-id`: port MAC address

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- The PPPoE server extracts the Line-ID tag from PPPoE discovery stage messages, and uses the Circuit-ID field of that tag as a NAS-Port-ID attribute in AAA access and accounting requests.

- The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-ID of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.

- Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-ID tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients using the `pppoe intermediate-agent vendor-tag strip` command.

- If the remote-id is unspecified, the port name will be used for this parameter. If the port name is not configured, the remote-id is set to the port MAC (yy-yy-yy-yy-yy-yy#), where # is the default delimiter.

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id ECS4620-28T
```

Console(config-if)#
**Authentication Commands**

### PPPoE Intermediate Agent

#### pppoe intermediate-agent

**port-format-type**

**remote-id-delimiter**

This command sets the remote-id delimiter for an interface. Use the `enable` keyword to enable the delimiter. Use the `no` form with the `enable` keyword to disable the delimiter. Use the `no` form without any keywords to restore the default settings.

**Syntax**

```
pppoe intermediate-agent port-format-type remote-id-delimiter

{ enable | ascii-code }
```

- `ascii-code` - ASCII character of delimiter. (Range: 0-255)

**Default Setting**

Disabled

ASCII code: 35 ("#")

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

If the delimiter is enabled and it occurs in the remote ID string, the string will be truncated at that point.

**Example**

This command enables the delimiter for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type remote-id-delimiter
Console(config-if)#
```

#### pppoe intermediate-agent

**trust**

This command sets an interface to trusted mode to indicate that it is connected to a PPPoE server. Use the `no` form to set an interface to untrusted mode.

**Syntax**

```
[no] pppoe intermediate-agent trust
```

**Default Setting**

Untrusted

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.
At least one trusted interface must be configured on the switch for the PPPoE IA to function.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent trust
Console(config-if)#
```

**pppoe intermediate-agent vendor-tag strip**

This command enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. Use the `no` form to disable this feature.

**Syntax**

```
[no] pppoe intermediate-agent vendor-tag strip
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

This command only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent vendor-tag strip
Console(config-if)#
```

**clear pppoe intermediate-agent statistics**

This command clears statistical counters for the PPPoE Intermediate Agent.

**Syntax**

```
clear pppoe intermediate-agent statistics interface [interface]
```

`interface`

- `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)

- `port-channel channel-id` (Range: 1-16)
**Chapter 7 | Authentication Commands**

**PPPoE Intermediate Agent**

**Command Mode**
Privileged Exec

**Example**

```
Console#clear pppoe intermediate-agent statistics
console#
```

**show pppoe intermediate-agent info**

This command displays configuration settings for the PPPoE Intermediate Agent.

**Syntax**

```
show pppoe intermediate-agent info [interface [interface]]

interface
  ethernet unit/port
    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)
```

**Command Mode**
Privileged Exec

**Example**

```
Console#show pppoe intermediate-agent info
PPPoE Intermediate Agent Global Status : Enabled
PPPoE Intermediate Agent Admin Access Node Identifier : 192.168.0.2
PPPoE Intermediate Agent Oper Access Node Identifier : 192.168.0.2
PPPoE Intermediate Agent Admin Generic Error Message :
PPPoE Intermediate Agent Oper Generic Error Message :
PPPoE Discover packet too large to process. Try reducing the number of tags added.

Console#show pppoe intermediate-agent info interface ethernet 1/1
Interface PPPoE IA Trusted Vendor-Tag Strip Admin Circuit-ID Admin Remote-ID
----------------- ----------------- ----------------- -------------------
Eth 1/2   Yes  Yes  Yes  1/2:vid 00-00-E8-94-40-02
R-ID Delimiter Delimiter ASCII  Oper Circuit-ID  Oper Remote-ID
----------------- ----------------- ----------------- -------------------
Yes 3 1/2:vid 00-00-E8-94-40-02

Console#
```
**show pppoe intermediate-agent statistics**

This command displays statistics for the PPPoE Intermediate Agent.

**Syntax**

```
show pppoe intermediate-agent statistics interface [interface]
```

- **interface**
  - `ethernet unit/port`
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)

**Command Mode**

Privileged Exec

**Example**

```
Console#show pppoe intermediate-agent statistics interface ethernet 1/1
Eth 1/1 statistics
-----------------------------------------------------------------------------
Received :        All       PADI       PADO       PADR       PADS       PADT
---------- ---------- ---------- ---------- ---------- ----------
                  3          0          0          0          0          3
Dropped  : Response from untrusted  Request towards untrusted  Malformed
-----------------------  -------------------------  ---------
                     0                          0          0

```

**Table 48: show pppoe intermediate-agent statistics - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PADI</td>
<td>PPPoE Active Discovery Initiation</td>
</tr>
<tr>
<td>PADO</td>
<td>PPPoE Active Discovery Offer</td>
</tr>
<tr>
<td>PADR</td>
<td>PPPoE Active Discovery Request</td>
</tr>
<tr>
<td>PADS</td>
<td>PPPoE Active Discovery Session-Confirmation</td>
</tr>
<tr>
<td>PADT</td>
<td>PPPoE Active Discovery Terminate</td>
</tr>
</tbody>
</table>
General Security Measures

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Port-based authentication using IEEE 802.1X is commonly used for these purposes. In addition to these methods, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

Table 49: General Security Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Security*</td>
<td>Configures secure addresses for a port</td>
</tr>
<tr>
<td>802.1X Port Authentication*</td>
<td>Configures host authentication on specific ports using 802.1X</td>
</tr>
<tr>
<td>Network Access*</td>
<td>Configures MAC authentication and dynamic VLAN assignment</td>
</tr>
<tr>
<td>Web Authentication*</td>
<td>Configures Web authentication</td>
</tr>
<tr>
<td>Access Control Lists*</td>
<td>Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)</td>
</tr>
<tr>
<td>DHCPv4 Snooping*</td>
<td>Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table</td>
</tr>
<tr>
<td>DHCPv6 Snooping*</td>
<td>Filters untrusted DHCPv6 messages on unsecure ports by building and maintaining a DHCPv6 snooping binding table</td>
</tr>
<tr>
<td>IPv4 Source Guard*</td>
<td>Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings</td>
</tr>
<tr>
<td>IPv6 Source Guard*</td>
<td>Filters IPv6 traffic on insecure ports for which the source address cannot be identified via DHCPv6 snooping nor static source bindings</td>
</tr>
<tr>
<td>ND Snooping</td>
<td>Maintains IPv6 prefix table and user address binding table which can be used for stateless address auto-configuration or for address filtering by IPv6 Source Guard</td>
</tr>
<tr>
<td>ARP Inspection</td>
<td>Validates the MAC-to-IP address bindings in ARP packets</td>
</tr>
<tr>
<td>DoS Protection</td>
<td>Protects against Denial-of-Service attacks</td>
</tr>
<tr>
<td>Port-based Traffic Segmentation</td>
<td>Configures traffic segmentation for different client sessions based on specified downlink and uplink ports</td>
</tr>
</tbody>
</table>

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, DHCP Snooping, and then IP Source Guard.
Port Security

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 50: Management IP Filter Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address-table static</td>
<td>Maps a static address to a port in a VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>mac-learning</td>
<td>Enables MAC address learning on the selected interface or VLAN</td>
<td>IC</td>
</tr>
<tr>
<td>port security</td>
<td>Configures a secure port</td>
<td>IC</td>
</tr>
<tr>
<td>show mac-address-table</td>
<td>Displays entries in the bridge-forwarding database</td>
<td>PE</td>
</tr>
<tr>
<td>show port security</td>
<td>Displays port security status and secure address count</td>
<td>PE</td>
</tr>
</tbody>
</table>

**mac-learning**  
This command enables MAC address learning on the selected interface. Use the **no** form to disable MAC address learning.

**Syntax**

```
[no] mac-learning
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet or Port Channel)

**Command Usage**

- The **no mac-learning** command immediately stops the switch from learning new MAC addresses on the specified port or trunk. Only incoming traffic with source addresses stored in the static address table will be accepted. Note that the dynamic addresses stored in the address table when MAC address learning
is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled.

- The mac-learning commands cannot be used if 802.1X Port Authentication has been globally enabled on the switch with the `dot1x system-auth-control` command, or if MAC Address Security has been enabled by the `port security` command on the same interface.

**Example**
The following example disables MAC address learning for port 2.

```plaintext
ES-3026(config)#interface ethernet 1/2
ES-3026(config-if)#no mac-learning
ES-3026(config-if)#
```

**Related Commands**
* show interfaces status (388)

**port security** This command enables or configures port security. Use the `no` form without any keywords to disable port security. Use the `no` form with the appropriate keyword to restore the default settings for a response to a security violation or for the maximum number of allowed addresses.

**Syntax**
```plaintext
port security
[[action {shutdown | trap | trap-and-shutdown}] |
[max-mac-count address-count]]
no port security [action | max-mac-count]
```

- **action** - Response to take when port security is violated.
  - shutdown - Disable port only.
  - trap - Issue SNMP trap message only.
  - trap-and-shutdown - Issue SNMP trap message and disable port.

- **max-mac-count**

  - **address-count** - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

**Default Setting**
- Status: Disabled
- Action: None
- Maximum Addresses: 0

**Command Mode**
- Interface Configuration (Ethernet)
Command Usage

- The default maximum number of MAC addresses allowed on a secure port is zero (that is, port security is disabled). To use port security, you must configure the maximum number of addresses allowed on a port using the `port security max-mac-count` command.

- When port security is enabled using the `port security` command, or the maximum number or allowed addresses is set to a value lower than the current limit after port security has been enabled, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- To configure the maximum number of address entries which can be learned on a port, and then specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. (The specified maximum address count is effective when port security is enabled or disabled.) Note that you can manually add additional secure addresses to a port using the `mac-address-table static` command. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.

- If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.

- If a port is disabled due to a security violation, it must be manually re-enabled using the `no shutdown` command.

- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
  - RSPAN and port security are mutually exclusive functions. If port security is enabled on a port, that port cannot be set as an RSPAN uplink port, source port, or destination port. Also, when a port is configured as an RSPAN uplink port, source port, or destination port, port security cannot be enabled on that port.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```
Related Commands

- show interfaces status (388)
- shutdown (383)
- mac-address-table static (460)

**show port security**  This command displays port security status and the secure address count.

**Syntax**

```
show port security [interface interface]
```

- **interface** - Specifies a port interface.
  - ethernet unit/port
    - **unit** - Unit identifier. (Range: 1)
    - **port** - Port number. (Range: 1-28/52)

**Command Mode**

Privileged Exec

**Example**

This example shows the port security settings and number of secure addresses for all ports.

```
Console#show port security
Global Port Security Parameters
Secure MAC Aging Mode : Disabled

Port Security Port Summary
Port         Port Security Port Status  Intrusion Action  MaxMacCnt  CurrMacCnt
--------------------------------------------------------------
Eth 1/1      Disabled       Secure/Down  None              0         2
Eth 1/2      Enabled        Secure/Up    None              10        0
Eth 1/3      Disabled       Secure/Down  None              0         0
Eth 1/4      Disabled       Secure/Down  None              0         0
Eth 1/5      Disabled       Secure/Down  None              0         0
```

**Table 51: show port security - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Security</td>
<td>The configured status (enabled or disabled).</td>
</tr>
<tr>
<td>Port Status</td>
<td>The operational status:</td>
</tr>
<tr>
<td></td>
<td>◦ Secure/Down – Port security is disabled.</td>
</tr>
<tr>
<td></td>
<td>◦ Secure/Up – Port security is enabled.</td>
</tr>
<tr>
<td></td>
<td>◦ Shutdown – Port is shut down due to a response to a port security violation.</td>
</tr>
<tr>
<td>Intrusion Action</td>
<td>The configured intrusion response.</td>
</tr>
</tbody>
</table>
The following example shows the port security settings and number of secure addresses for a specific port. The Last Intrusion MAC and Last Time Detected Intrusion MAC fields show information about the last detected intrusion MAC address. These fields are not applicable if no intrusion has been detected or port security is disabled. The MAC Filter ID field is configured by the `network-access port-mac-filter` command. If this field displays Disabled, then any unknown source MAC address can be learned as a secure MAC address. If it displays a filter identifier, then only source MAC address entries in MAC Filter table can be learned as secure MAC addresses.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC Aging Mode : Disabled

Port Security Details
  Port : 1/2
  Port Security : Enabled
  Port Status : Secure/Up
  Intrusion Action : None
  Max MAC Count : 0
  Current MAC Count : 0
  MAC Filter : Disabled
  Last Intrusion MAC : NA
  Last Time Detected Intrusion MAC : NA
Console#
```

This example shows information about a detected intrusion.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC Aging Mode : Disabled

Port Security Details
  Port : 1/2
  Port Security : Enabled
  Port Status : Secure/Up
  Intrusion Action : None
  Max MAC Count : 0
  Current MAC Count : 0
  MAC Filter : Disabled
  Last Intrusion MAC : 00-10-22-00-00-01
  Last Time Detected Intrusion MAC : 2010/7/29 15:13:03
Console#
```
Network Access (MAC Address Authentication)

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

**Table 52: Network Access Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-access aging</td>
<td>Enables MAC address aging</td>
<td>GC</td>
</tr>
<tr>
<td>network-access mac-filter</td>
<td>Adds a MAC address to a filter table</td>
<td>GC</td>
</tr>
<tr>
<td>mac-authentication reauth-time</td>
<td>Sets the time period after which a connected MAC address must be re-authenticated</td>
<td>GC</td>
</tr>
<tr>
<td>network-access dynamic-qos</td>
<td>Enables the dynamic quality of service feature</td>
<td>IC</td>
</tr>
<tr>
<td>network-access dynamic-vlan</td>
<td>Enables dynamic VLAN assignment from a RADIUS server</td>
<td>IC</td>
</tr>
<tr>
<td>network-access guest-vlan</td>
<td>Specifies the guest VLAN</td>
<td>IC</td>
</tr>
<tr>
<td>network-access link-detection</td>
<td>Enables the link detection feature</td>
<td>IC</td>
</tr>
<tr>
<td>network-access link-detection link-down</td>
<td>Configures the link detection feature to detect and act upon link-down events</td>
<td>IC</td>
</tr>
<tr>
<td>network-access link-detection link-up</td>
<td>Configures the link detection feature to detect and act upon link-up events</td>
<td>IC</td>
</tr>
<tr>
<td>network-access link-detection link-up-down</td>
<td>Configures the link detection feature to detect and act upon both link-up and link-down events</td>
<td>IC</td>
</tr>
<tr>
<td>network-access max-mac-count</td>
<td>Sets the maximum number of MAC addresses that can be authenticated on a port via all forms of authentication</td>
<td>IC</td>
</tr>
<tr>
<td>network-access mode</td>
<td>Enables MAC authentication on an interface</td>
<td>IC</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>Determines the port response when a connected host fails MAC authentication.</td>
<td>IC</td>
</tr>
<tr>
<td>mac-authentication max-mac-count</td>
<td>Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication</td>
<td>IC</td>
</tr>
<tr>
<td>clear network-access</td>
<td>Clears authenticated MAC addresses from the address table</td>
<td>PE</td>
</tr>
<tr>
<td>show network-access</td>
<td>Displays the MAC authentication settings for port interfaces</td>
<td>PE</td>
</tr>
<tr>
<td>show network-access mac-address-table</td>
<td>Displays information for entries in the secure MAC address table</td>
<td>PE</td>
</tr>
<tr>
<td>show network-access mac-filter</td>
<td>Displays information for entries in the MAC filter tables</td>
<td>PE</td>
</tr>
</tbody>
</table>
**network-access aging**  Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the `no` form of this command to disable address aging.

**Syntax**

```
[no] network-access aging
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the `mac-address-table aging-time` command.

- This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 249).

- The maximum number of secure MAC addresses supported for the switch system is 1024.

**Example**

```
Console(config-if)#network-access aging
```

**network-access mac-filter**  Use this command to add a MAC address into a filter table. Use the `no` form of this command to remove the specified MAC address.

**Syntax**

```
[no] network-access mac-filter filter-id
mac-address mac-address [mask mask-address]
```

- `filter-id` - Specifies a MAC address filter table. (Range: 1-64)
- `mac-address` - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)
- `mask` - Specifies a MAC address bit mask for a range of addresses.

**Default Setting**

Disabled
Command Mode
Global Configuration

Command Usage
◆ Specified addresses are exempt from network access authentication.

◆ This command is different from configuring static addresses with the `mac-address-table static` command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the `network-access port-mac-filter` command.

◆ Up to 64 filter tables can be defined.

◆ There is no limitation on the number of entries that can entered in a filter table.

Example

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

mac-authentication reauth-time

Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the `no` form of this command to restore the default value.

Syntax

```
mac-authentication reauth-time seconds

no mac-authentication reauth-time

seconds - The reauthentication time period. (Range: 120-1000000 seconds)
```

Default Setting

1800

Command Mode
Global Configuration

Command Usage
◆ The reauthentication time is a global setting and applies to all ports.

◆ When the reauthentication time expires for a secure MAC address it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected.

Example

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```
**network-access dynamic-qos** Use this command to enable the dynamic QoS feature for an authenticated port. Use the `no` form to restore the default.

**Syntax**

```
[no] network-access dynamic-qos
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration

**Command Usage**

- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The “Filter-ID” attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

**Table 53: Dynamic QoS Profiles**

<table>
<thead>
<tr>
<th>Profile</th>
<th>Attribute Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiffServ</td>
<td><code>service-policy-in=policy-map-name</code></td>
<td><code>service-policy-in=p1</code></td>
</tr>
<tr>
<td>Rate Limit</td>
<td><code>rate-limit-input=rate (Kbps)</code></td>
<td><code>rate-limit-input=100 (Kbps)</code></td>
</tr>
<tr>
<td></td>
<td><code>rate-limit-output=rate (Kbps)</code></td>
<td><code>rate-limit-output=200 (Kbps)</code></td>
</tr>
<tr>
<td>802.1p</td>
<td><code>switchport-priority-default=value</code></td>
<td><code>switchport-priority-default=2</code></td>
</tr>
<tr>
<td>IP ACL</td>
<td><code>ip-access-group-in=ip-acl-name</code></td>
<td><code>ip-access-group-in=ipv4acl</code></td>
</tr>
<tr>
<td>IPv6 ACL</td>
<td><code>ipv6-access-group-in=ipv6-acl-name</code></td>
<td><code>ipv6-access-group-in=ipv6acl</code></td>
</tr>
<tr>
<td>MAC ACL</td>
<td><code>mac-access-group-in=mac-acl-name</code></td>
<td><code>mac-access-group-in=macAcl</code></td>
</tr>
</tbody>
</table>

- When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.

**Note:** Any configuration changes for dynamic QoS are not saved to the switch configuration file.
Example
The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

**network-access dynamic-vlan**

Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

**Syntax**

```
[no] network-access dynamic-vlan
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration

**Command Usage**

◆ When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch. GVRP is not used to create the VLANs.

◆ The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.

◆ If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.

◆ When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

**Example**

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```
**network-access guest-vlan**

Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication or MAC authentication is rejected. Use the `no` form of this command to disable guest VLAN assignment.

**Syntax**

```
network-access guest-vlan vlan-id
no network-access guest-vlan
```

- `vlan-id` - VLAN ID (Range: 1-4094)

**Default Setting**

Disabled

**Command Mode**

Interface Configuration

**Command Usage**

- The VLAN to be used as the guest VLAN must be defined and set as active (See the `vlan database` command).

- When used with 802.1X authentication, the intrusion-action must be set for "guest-vlan" to be effective (see the `dot1x intrusion-action` command).

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

**network-access link-detection**

Use this command to enable link detection for the selected port. Use the `no` form of this command to restore the default.

**Syntax**

```
[no] network-access link-detection
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```
network-access link-detection link-down

Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the no form of this command to disable this feature.

Syntax

```
network-access link-detection link-down
action [shutdown | trap | trap-and-shutdown]
```

```
no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.
```

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link-up

Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the no form of this command to disable this feature.

Syntax

```
network-access link-detection link-up
action [shutdown | trap | trap-and-shutdown]
```

```
no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.
```

Default Setting

Disabled

Command Mode

Interface Configuration
Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

**network-access link-detection link-up-down**

Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

**Syntax**

```
network-access link-detection link-up-down action [shutdown | trap | trap-and-shutdown]
no network-access link-detection
```

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable the port.

**Default Setting**

Disabled

**Command Mode**

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

**network-access max-mac-count**

Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the **no** form of this command to restore the default.

**Syntax**

```
network-access max-mac-count count
no network-access max-mac-count
```

- **count** - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 1-2048)

**Default Setting**

1024
Chapter 8 | General Security Measures  
Network Access (MAC Address Authentication)

Command Mode  
Interface Configuration

Command Usage  
The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

Example

```
Console(config-if)#network-access max-mac-count 5  
Console(config-if)#
```

**network-access mode mac-authentication**  
Use this command to enable network access authentication on a port. Use the **no** form of this command to disable network access authentication.

Syntax

```
[no] network-access mode mac-authentication
```

Default Setting  
Disabled

Command Mode  
Interface Configuration

Command Usage

- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.

- On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).

- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.

-Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.

- MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.

- MAC authentication cannot be configured on trunk ports.
When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.

The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the “Tunnel-Private-Group-ID” attribute. The VLAN list can contain multiple VLAN identifiers in the format “1u,2t,” where “u” indicates untagged VLAN and “t” tagged VLAN. The “Tunnel-Type” attribute should be set to “VLAN,” and the “Tunnel-Medium-Type” attribute set to “802.”

Example

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

```
network-access
port-mac-filter
```

Use this command to enable the specified MAC address filter. Use the `no` form of this command to disable the specified MAC address filter.

Syntax

```
network-access port-mac-filter filter-id
```

```
o network-access port-mac-filter
```

`filter-id` - Specifies a MAC address filter table. (Range: 1-64)

Default Setting

None

Command Mode

Interface Configuration

Command Mode

Entries in the MAC address filter table can be configured with the `network-access mac-filter` command.

Only one filter table can be assigned to a port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```
**mac-authentication intrusion-action** Use this command to configure the port response to a host MAC authentication failure. Use the **no** form of this command to restore the default.

**Syntax**

```
mac-authentication intrusion-action {block traffic | pass traffic}
no mac-authentication intrusion-action
```

**Default Setting**
Block Traffic

**Command Mode**
Interface Configuration

**Example**

```
Console(config-if)#mac-authentication intrusion-action block-traffic
Console(config-if)#
```

**mac-authentication max-mac-count** Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the **no** form of this command to restore the default.

**Syntax**

```
mac-authentication max-mac-count count
no mac-authentication max-mac-count
```

**Default Setting**
1024

**Command Mode**
Interface Configuration

**Example**

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```
clear network-access  Use this command to clear entries from the secure MAC addresses table.

Syntax

```
clear network-access mac-address-table [static | dynamic]
  [address mac-address] [interface interface]
```

- **static** - Specifies static address entries.
- **dynamic** - Specifies dynamic address entries.
- **mac-address** - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)
- **interface** - Specifies a port interface.

```
ethernet unit/port
```

- **unit** - Unit number. (Range: 1)
- **port** - Port number. (Range: 1-28/52)

Default Setting
None

Command Mode
Privileged Exec

Example

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

show network-access  Use this command to display the MAC authentication settings for port interfaces.

Syntax

```
show network-access [interface interface]
```

- **interface** - Specifies a port interface.

```
ethernet unit/port
```

- **unit** - Unit identifier. (Range: 1)
- **port** - Port number. (Range: 1-28/52)

Default Setting
Displays the settings for all interfaces.

Command Mode
Privileged Exec
Example

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time : 1800
MAC Address Aging : Disabled

Port : 1/1
MAC Authentication : Disabled
MAC Authentication Intrusion Action : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts : 2048
Dynamic VLAN Assignment : Enabled
Dynamic QoS Assignment : Disabled
MAC Filter ID : Disabled
Guest VLAN : Disabled
Link Detection : Disabled
Detection Mode : Link-down
Detection Action : Trap
Console#
```

**show network-access mac-address-table**

Use this command to display secure MAC address table entries.

**Syntax**

```
show network-access mac-address-table [static | dynamic]
[address mac-address [mask]] [interface interface] [sort {address | interface}]

static - Specifies static address entries.
dynamic - Specifies dynamic address entries.
mac-address - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)
mask - Specifies a MAC address bit mask for filtering displayed addresses.
interface - Specifies a port interface.

ethernet unit/port

unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)

sort - Sorts displayed entries by either MAC address or interface.
```

**Default Setting**
Displays all filters.

**Command Mode**
Privileged Exec

**Command Usage**
When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don’t care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-
Web Authentication

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.
Web Authentication

Note: RADIUS authentication must be activated and configured for the web authentication feature to work properly (see “Authentication Sequence” on page 208).

Note: Web authentication cannot be configured on trunk ports.

web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the no form to restore the default.

Syntax

```
web-auth login-attempts count
no web-auth login-attempts
```

count - The limit of allowed failed login attempts. (Range: 1-3)

Default Setting
3 login attempts

Command Mode
Global Configuration
**web-auth quiet-period**  This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

**Syntax**

```
web-auth quiet-period time
no web-auth quiet period
```

`time` - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

**Default Setting**

60 seconds

**Command Mode**

Global Configuration

**Example**

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

**web-auth session-timeout**  This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

**Syntax**

```
web-auth session-timeout timeout
no web-auth session timeout
```

`timeout` - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds, or 0 for disabled)

**Default Setting**

3600 seconds

**Command Mode**

Global Configuration
Example

```plaintext
Console(config)#web-auth session-timeout 1800
Console(config)#
```

**web-auth system-auth-control**

This command globally enables web authentication for the switch. Use the `no` form to restore the default.

**Syntax**

```
[no] web-auth system-auth-control
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

Both `web-auth system-auth-control` for the switch and `web-auth` for an interface must be enabled for the web authentication feature to be active.

Example

```plaintext
Console(config)#web-auth system-auth-control
Console(config)#
```

**web-auth**

This command enables web authentication for an interface. Use the `no` form to restore the default.

**Syntax**

```
[no] web-auth
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration

**Command Usage**

Both `web-auth system-auth-control` for the switch and `web-auth` for a port must be enabled for the web authentication feature to be active.
**web-auth re-authenticate (Port)**  
This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

**Syntax**
```
web-auth re-authenticate interface interface
interface - Specifies a port interface.
    ethernet unit/port
        unit - This is unit 1.
        port - Port number. (Range: 1-28/52)
```

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**
```
Console#web-auth re-authenticate interface ethernet 1/2
Console#  
```

**web-auth re-authenticate (IP)**  
This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

**Syntax**
```
web-auth re-authenticate interface ip
interface - Specifies a port interface.
    ethernet unit/port
        unit - This is unit 1.
        port - Port number. (Range: 1-28/52)
    ip - IPv4 formatted IP address
```

**Default Setting**
None

**Command Mode**
Privileged Exec
Example

```
Example
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

**show web-auth**

This command displays global web authentication parameters.

**Command Mode**

Privileged Exec

**Example**

```
Example
Console#show web-auth

Global Web-Auth Parameters

  System Auth Control : Enabled
  Session Timeout     : 3600
  Quiet Period        : 60
  Max Login Attempts  : 3

Console#
```

**show web-auth interface**

This command displays interface-specific web authentication parameters and statistics.

**Syntax**

```
show web-auth interface interface

interface - Specifies a port interface.

ethernet unit/port

  unit - This is unit 1.

  port - Port number. (Range: 1-28/52)
```

**Command Mode**

Privileged Exec

**Example**

```
Example
Console#show web-auth interface ethernet 1/2

Web Auth Status       : Enabled

Host Summary

<table>
<thead>
<tr>
<th>IP address</th>
<th>Web-Auth-State</th>
<th>Remaining-Session-Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>Authenticated</td>
<td>295</td>
</tr>
<tr>
<td>1.1.1.2</td>
<td>Authenticated</td>
<td>111</td>
</tr>
</tbody>
</table>

Console#
```
show web-auth summary

This command displays a summary of web authentication port parameters and statistics.

Command Mode
Privileged Exec

Example

Console#show web-auth summary

Global Web-Auth Parameters

<table>
<thead>
<tr>
<th>System Auth Control</th>
<th>Port</th>
<th>Status</th>
<th>Authenticated Host Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>1/ 1</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1/ 2</td>
<td>Enabled</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>1/ 3</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1/ 4</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1/ 5</td>
<td>Disabled</td>
<td>0</td>
</tr>
</tbody>
</table>

DHCPv4 Snooping

DHCPv4 snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv4 snooping.

Table 55: DHCP Snooping Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping</td>
<td>Enables DHCP snooping globally</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping information</td>
<td>Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping information</td>
<td>Disables use of sub-type and sub-length for the CID/RID in Option 82 information</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping information</td>
<td>Sets the remote ID to the switch's IP address, MAC address, arbitrary string, or TR-101 compliant node identifier</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping information</td>
<td>Sets the information option policy for DHCP client packets that include Option 82 information</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping limit rate</td>
<td>Sets the maximum number of DHCP packets that can be trapped for DHCP snooping</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping verify</td>
<td>Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping vlan</td>
<td>Enables DHCP snooping on the specified VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>ip dhcp snooping information</td>
<td>Enables or disables the use of DHCP Option 82 information circuit-id suboption</td>
<td>IC</td>
</tr>
</tbody>
</table>
### ip dhcp snooping

This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

**Syntax**

```
[no] ip dhcp snooping
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or firewall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the `ip dhcp snooping vlan` command, DHCP messages received on an untrusted interface (as specified by the `no ip dhcp snooping trust` command) from a device not listed in the DHCP snooping table will be dropped.

- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- Filtering rules are implemented as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping trust</td>
<td>Configures the specified interface as trusted</td>
<td>IC</td>
</tr>
<tr>
<td>clear ip dhcp snooping binding</td>
<td>Clears DHCP snooping binding table entries from RAM</td>
<td>PE</td>
</tr>
<tr>
<td>clear ip dhcp snooping database flash</td>
<td>Removes all dynamically learned snooping entries from flash memory.</td>
<td>PE</td>
</tr>
<tr>
<td>ip dhcp snooping database flash</td>
<td>Writes all dynamically learned snooping entries to flash memory</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp snooping</td>
<td>Shows the DHCP snooping configuration settings</td>
<td>PE</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Shows the DHCP snooping binding table entries</td>
<td>PE</td>
</tr>
</tbody>
</table>

Table 55: DHCP Snooping Commands
- If global DHCP snooping is disabled, all DHCP packets are forwarded.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
  - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
  - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
  - If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the `ip dhcp snooping verify mac-address` command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client’s hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
  - If the DHCP packet is not a recognizable type, it is dropped.
  - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
  - If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the `ip dhcp snooping trust` command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.
Example
This example enables DHCP snooping globally for the switch.

```
Console(config)#ip dhcp snooping
Console(config)#
```

Related Commands
ip dhcp snooping vlan (304)
ip dhcp snooping trust (306)

**ip dhcp snooping information option**

This command enables the use of DHCP Option 82 information for the switch, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the `no` form without any keywords to disable this function, the no form with the encode no-subtype keyword to enable use of sub-type and sub-length in CID/RID fields, or the `no` form with the `remote-id` keyword to set the remote ID to the switch’s MAC address encoded in hexadecimal.

**Syntax**

```
ip dhcp snooping information option
  [encode no-subtype] [remote-id (ip-address [encode {ascii | hex}]) | mac-address [encode {ascii | hex}] | string string]]
no ip dhcp snooping information option [encode no-subtype]
  [remote-id [ip-address encode] | [mac-address encode]]
```

- **encode no-subtype** - Disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.
- **mac-address** - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch’s CPU).
- **ip-address** - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).
- **encode** - Indicates encoding in ASCII or hexadecimal.
- **string** - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)

**Default Setting**
Option 82: Disabled
CID/RID sub-type: Enabled
Remote ID: MAC address (hexadecimal)

**Command Mode**
Global Configuration

**Command Usage**
- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows
compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.

◆ When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server.

◆ When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.

◆ DHCP snooping must be enabled for the DHCP Option 82 information to be inserted into packets. When enabled, the switch will only add/remove option 82 information in incoming DCHP packets but not relay them. Packets are processed as follows:
  ■ If an incoming packet is a DHCP request packet with option 82 information, it will modify the option 82 information according to settings specified with `ip dhcp snooping information policy` command.
  ■ If an incoming packet is a DHCP request packet without option 82 information, enabling the DHCP snooping information option will add option 82 information to the packet.
  ■ If an incoming packet is a DHCP reply packet with option 82 information, enabling the DHCP snooping information option will remove option 82 information from the packet.

**Example**
This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

**ip dhcp snooping information option encode no-subtype**
This command disables the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID) in Option 82 information generated by the switch. Use the `no` form to enable the use of these fields.

**Syntax**
```
[no] ip dhcp snooping information option encode no-subtype
```

**Default Setting**
Enabled

**Command Mode**
Global Configuration
Chapter 8 | General Security Measures

DHCPv4 Snooping

**Command Usage**

See the Command Usage section under the `ip dhcp snooping information option circuit-id` command for a description of how these fields are included in TR-101 syntax.

**EXAMPLE**

This example enables the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID).

```
Console(config)#no ip dhcp snooping information option encode no-subtype
Console(config)#
```

**ip dhcp snooping information option remote-id**

This command sets the remote ID to the switch's IP address, MAC address, arbitrary string, or TR-101 compliant node identifier. Use the `no` form to restore the default setting.

**Syntax**

```
ip dhcp snooping information option remote-id
    {ip-address [encode {ascii | hex}] | mac-address [encode {ascii | hex}] | string |
    tr101 node-identifier {ip | sysname}]
```

```
o ip dhcp snooping information option remote-id
    [ip-address encode] | [mac-address encode]
```

- **mac-address** - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch's CPU).
- **ip-address** - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).
- **encode** - Indicates encoding in ASCII or hexadecimal.
- **string** - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)
- **tr101 node-identifier** - The remote ID generated by the switch is based on TR-101 syntax (R-124, Access_Node_ID).
  - **ip** - Specifies the switch's IP address as the node identifier.
  - **sysname** - Specifies the system name as the node identifier.

**Default Setting**

MAC address (hexadecimal)

**Command Mode**

Global Configuration
**Example**
This example sets the remote ID to the switch's IP address.

```
Console(config)#ip dhcp snooping information option remote-id tr101 node-identifier ip
Console(config)#
```

**ip dhcp snooping information policy**
This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information. Use the **no** form to restore the default setting.

**Syntax**
```
ip dhcp snooping information policy {drop | keep | replace}
```

- **drop** - Drops the client's request packet instead of relaying it.
- **keep** - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
- **replace** - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

**Default Setting**
replace

**Command Mode**
Global Configuration

**Command Usage**
When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

**Example**
```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```
**ip dhcp snooping limit rate**  
This command sets the maximum number of DHCP packets that can be trapped by the switch for DHCP snooping. Use the **no** form to restore the default setting.

**Syntax**

```
ip dhcp snooping limit rate rate
no dhcp snooping limit rate
```

*rate* - The maximum number of DHCP packets that may be trapped for DHCP snooping. (Range: 1-2048 packets/second)

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Example**

This example sets the DHCP snooping rate limit to 100 packets per second.

```
Console(config)#ip dhcp snooping limit rate 100
Console(config)#
```

**ip dhcp snooping verify mac-address**  
This command verifies the client’s hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

**Syntax**

```
[no] ip dhcp snooping verify mac-address
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Command Usage**

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client’s hardware address in the DHCP packet, the packet is dropped.
Example
This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

Related Commands
- `ip dhcp snooping` (297)
- `ip dhcp snooping vlan` (304)
- `ip dhcp snooping trust` (306)

**ip dhcp snooping vlan**
This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

**Syntax**
```
[no] ip dhcp snooping vlan vlan-id
```

- `vlan-id` - ID of a configured VLAN (Range: 1-4094)

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
- When DHCP snooping is enabled globally using the `ip dhcp snooping` command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the `ip dhcp snooping trust` command.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

**Example**
This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```
Related Commands
ip dhcp snooping (297)
ip dhcp snooping trust (306)

**ip dhcp snooping information option circuit-id**

This command specifies DHCP Option 82 circuit-id suboption information. Use the `no` form to use the default settings.

**Syntax**

```
ip dhcp snooping information option circuit-id string

no dhcp snooping information option circuit-id

string - An arbitrary string inserted into the circuit identifier field.
(Range: 1-32 characters)
```

**Default Setting**

VLAN-Unit-Port

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. DHCP Option 82 allows compatible DHCP servers to use the information when assigning IP addresses, to set other services or policies for clients. For more information of this process, refer to the Command Usage section under the `ip dhcp snooping information option circuit-id` command.

- Option 82 information generated by the switch is based on TR-101 syntax as shown below:

<table>
<thead>
<tr>
<th>82</th>
<th>3-69</th>
<th>1</th>
<th>1-67</th>
<th>x1</th>
<th>x2</th>
<th>x3</th>
<th>x4</th>
<th>x5</th>
<th>x63</th>
</tr>
</thead>
<tbody>
<tr>
<td>opt82</td>
<td>opt-len</td>
<td>sub-opt1</td>
<td>string-len</td>
<td>R-124 string</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The circuit identifier used by this switch starts at sub-option1 and goes to the end of the R-124 string. The R-124 string includes the following information:

- sub-type - Distinguishes different types of circuit IDs.
- sub-length - Length of the circuit ID type
- access node identifier - ASCII string. Default is the MAC address of the switch's CPU. This field is set by the `ip dhcp snooping information option circuit-id` command,
- eth - The second field is the fixed string "eth"
- slot - The slot represents the stack unit for this system.
port - The port which received the DHCP request. If the packet arrives over a trunk, the value is the ifIndex of the trunk.

- vlan - Tag of the VLAN which received the DHCP request.

Note that the sub-type and sub-length fields can be enabled or disabled using the ip dhcp snooping information option command.

- The **ip dhcp snooping information option circuit-id** command can be used to modify the default settings described above.

**Example**

This example sets the DHCP Snooping Information circuit-id suboption string.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping information option circuit-id string mv2
Console(config-if)#
```

**ip dhcp snooping trust**

This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

**Syntax**

```
[no] ip dhcp snooping trust
```

**Default Setting**

All interfaces are untrusted

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.

- Set all ports connected to DHCP servers within the local network or firewall to trusted, and all other ports outside the local network or firewall to untrusted.

- When DHCP snooping is enabled globally using the **ip dhcp snooping** command, and enabled on a VLAN with **ip dhcp snooping vlan** command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.

- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
◆ Additional considerations when the switch itself is a DHCP client – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

**Example**
This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

**Related Commands**
ip dhcp snooping (297)
ip dhcp snooping vlan (304)

clear ip dhcp snooping binding
This command clears DHCP snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

**Syntax**
```
clear ip dhcp snooping binding [mac-address vlan vlan-id]
```

- `mac-address` - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)
- `vlan-id` - ID of a configured VLAN (Range: 1-4094)

**Command Mode**
Privileged Exec

**Example**
```
Console#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console#
```

clear ip dhcp snooping database flash
This command removes all dynamically learned snooping entries from flash memory.

**Command Mode**
Privileged Exec

**Example**
```
Console#clear ip dhcp snooping database flash
Console#
```
**ip dhcp snooping database flash**  
This command writes all dynamically learned snooping entries to flash memory.

**Command Mode**  
Privileged Exec

**Command Usage**  
This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

**Example**

```
Console#ip dhcp snooping database flash
Console#
```

**show ip dhcp snooping**  
This command shows the DHCP snooping configuration settings.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Option Sub-option Format: extra subtype included
DHCP Snooping Information Option Remote ID: MAC Address (hex encoded)
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
DHCP Snooping rate limit: unlimited

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Circuit-ID mode</th>
<th>Circuit-ID Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>No</td>
<td>VLAN-Unit-Port</td>
<td>---</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>No</td>
<td>VLAN-Unit-Port</td>
<td>---</td>
</tr>
<tr>
<td>Eth 1/3</td>
<td>No</td>
<td>VLAN-Unit-Port</td>
<td>---</td>
</tr>
<tr>
<td>Eth 1/4</td>
<td>No</td>
<td>VLAN-Unit-Port</td>
<td>---</td>
</tr>
<tr>
<td>Eth 1/5</td>
<td>No</td>
<td>VLAN-Unit-Port</td>
<td>---</td>
</tr>
</tbody>
</table>
```

---

---
This command shows the DHCP snooping binding table entries.

**Command Mode**
Privileged Exec

**Example**

```
Console#show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec) Type                 VLAN Interface
----------------- --------------- ---------- -------------------- ---- ----─
11-22-33-44-55-66 192.168.0.99             0 Dynamic-DHCP-SNP       1 Eth 1/5
Console#
```

DHCPv6 Snooping

DHCPv6 snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv6 snooping.

**Table 57: DHCP Snooping Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp snooping</td>
<td>Enables DHCPv6 snooping globally</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping option remote-id</td>
<td>Enables insertion of DHCPv6 Option 37 relay agent remote-id</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping option remote-id policy</td>
<td>Sets the information option policy for DHCPv6 client</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>packets that include Option 37 information</td>
<td></td>
</tr>
<tr>
<td>ipv6 dhcp snooping vlan</td>
<td>Enables DHCPv6 snooping on the specified VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp snooping max-binding</td>
<td>Sets the maximum number of entries which can be</td>
<td>IC</td>
</tr>
<tr>
<td></td>
<td>stored in the binding database for an interface</td>
<td></td>
</tr>
<tr>
<td>ipv6 dhcp snooping trust</td>
<td>Configures the specified interface as trusted</td>
<td>IC</td>
</tr>
<tr>
<td>clear ipv6 dhcp snooping binding</td>
<td>Clears DHCPv6 snooping binding table entries from RAM</td>
<td>PE</td>
</tr>
<tr>
<td>clear ipv6 dhcp snooping statistics</td>
<td>Clears statistical counters for DHCPv6 snooping client, server and</td>
<td>PE</td>
</tr>
<tr>
<td></td>
<td>relay packets</td>
<td></td>
</tr>
<tr>
<td>show ipv6 dhcp snooping</td>
<td>Shows the DHCPv6 snooping configuration settings</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping binding</td>
<td>Shows the DHCPv6 snooping binding table entries</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping statistics</td>
<td>Shows statistics for DHCPv6 snooping client, server and relay packets</td>
<td>PE</td>
</tr>
</tbody>
</table>
ipv6 dhcp snooping  This command enables DHCPv6 snooping globally. Use the **no** form to restore the default setting.

**Syntax**

```
[no] ipv6 dhcp snooping
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- Network traffic may be disrupted when malicious DHCPv6 messages are received from an outside source. DHCPv6 snooping is used to filter DHCPv6 messages received on an unsecure interface from outside the network or firewall. When DHCPv6 snooping is enabled globally by this command, and enabled on a VLAN interface by the `ipv6 dhcp snooping vlan` command, DHCP messages received on an untrusted interface (as specified by the `no ipv6 dhcp snooping trust` command) from a device not listed in the DHCPv6 snooping table will be dropped.

- When enabled, DHCPv6 messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCPv6 snooping.

- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IPv6 address, lease time, binding type, VLAN identifier, and port identifier.

- When DHCPv6 snooping is enabled, the rate limit for the number of DHCPv6 messages that can be processed by the switch is 100 packets per second. Any DHCPv6 packets in excess of this limit are dropped.

- Filtering rules are implemented as follows:
  
  - If global DHCPv6 snooping is disabled, all DHCPv6 packets are forwarded.
  
  - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCPv6 packet is received, DHCPv6 packets are forwarded for a trusted port as described below.
  
  - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, DHCP packets are processed according to message type as follows:

    **DHCP Client Packet**

    - Request: Update entry in binding cache, recording client’s DHCPv6 Unique Identifier (DUID), server’s DUID, Identity Association (IA) type, IA
Identifier, and address (4 message exchanges to get IPv6 address), and forward to trusted port.

- **Solicit:** Add new entry in binding cache, recording client’s DUID, IA type, IA ID (2 message exchanges to get IPv6 address with rapid commit option, otherwise 4 message exchanges), and forward to trusted port.

- **Decline:** If no matching entry is found in binding cache, drop this packet.

- **Renew, Rebind, Release, Confirm:** If no matching entry is found in binding cache, drop this packet.

- **If the DHCPv6 packet is not a recognizable type, it is dropped.**

If a DHCPv6 packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

**DHCP Server Packet**

- If a DHCP server packet is received on an untrusted port, drop this packet and add a log entry in the system.

- If a DHCPv6 Reply packet is received from a server on a trusted port, it will be processed in the following manner:

  A. **Check if IPv6 address in IA option is found in binding table:**
     - If yes, continue to C.
     - If not, continue to B.

  B. **Check if IPv6 address in IA option is found in binding cache:**
     - If yes, continue to C.
     - If not, check failed, and forward packet to trusted port.

  C. **Check status code in IA option:**
     - If successful, and entry is in binding table, update lease time and forward to original destination.
     - If successful, and entry is in binding cache, move entry from binding cache to binding table, update lease time and forward to original destination.
     - Otherwise, remove binding entry. and check failed.

- If a DHCPv6 Relay packet is received, check the relay message option in Relay-Forward or Relay-Reply packet, and process client and server packets as described above.

- If DHCPv6 snooping is globally disabled, all dynamic bindings are removed from the binding table.
◆ Additional considerations when the switch itself is a DHCPv6 client – The port(s) through which the switch submits a client request to the DHCPv6 server must be configured as trusted (using the `ipv6 dhcp snooping trust` command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCPv6 server. Also, when the switch sends out DHCPv6 client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCPv6 server, any packets received from untrusted ports are dropped.

**Example**
This example enables DHCPv6 snooping globally for the switch.

```
Console(config)#ipv6 dhcp snooping
Console(config)#
```

**Related Commands**
`ipv6 dhcp snooping vlan (314)`
`ipv6 dhcp snooping trust (315)`

**ipv6 dhcp snooping option remote-id**
This command enables the insertion of remote-id option 37 information into DHCPv6 client messages. Remote-id option information such as the port attached to the client, DUID, and VLAN ID is used by the DHCPv6 server to assign preassigned configuration data specific to the DHCPv6 client. Use the `no` form of the command to disable this function.

**Syntax**
```
[no] ipv6 dhcp snooping option remote-id
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
◆ DHCPv6 provides a relay mechanism for sending information about the switch and its DHCPv6 clients to the DHCPv6 server. Known as DHCPv6 Option 37, it allows compatible DHCPv6 servers to use the information when assigning IP addresses, or to set other services or policies for clients.

◆ When DHCPv6 Snooping Information Option 37 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCPv6 request packets forwarded by the switch and in reply packets sent back from the DHCPv6 server.

◆ When the DHCPv6 Snooping Option 37 is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address.
DHCPv6 client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.

- DHCPv6 snooping must be enabled for the DHCPv6 Option 37 information to be inserted into packets. When enabled, the switch will either drop, keep or remove option 37 information in incoming DCHPv6 packets. Packets are processed as follows:
  - If an incoming packet is a DHCPv6 request packet with option 37 information, it will modify the option 37 information according to settings specified with `ipv6 dhcp snooping option remote-id policy` command.
  - If an incoming packet is a DHCPv6 request packet without option 37 information, enabling the DHCPv6 snooping information option will add option 37 information to the packet.
  - If an incoming packet is a DHCPv6 reply packet with option 37 information, enabling the DHCPv6 snooping information option will remove option 37 information from the packet.

- When this switch inserts Option 37 information in DHCPv6 client request packets, the switch’s MAC address (hexadecimal) is used for the remote ID.

**Example**
This example enables the DHCPv6 Snooping Remote-ID Option.

```
Console(config)#ipv6 dhcp snooping option remote-id
Console(config)#
```

**ipv6 dhcp snooping option remote-id policy**
This command sets the remote-id option policy for DHCPv6 client packets that include Option 37 information. Use the no form to disable this function.

**Syntax**

```
ipv6 dhcp snooping option remote-id policy {drop | keep | replace}
```

**no ipv6 dhcp snooping option remote-id policy**

- **drop** - Drops the client’s request packet instead of relaying it.
- **keep** - Retains the Option 37 information in the client request, and forwards the packets to trusted ports.
- **replace** - Replaces the Option 37 remote-ID in the client’s request with the relay agent’s remote-ID (when DHCPv6 snooping is enabled), and forwards the packets to trusted ports.

**Default Setting**
drop

**Command Mode**
Global Configuration
Chapter 8 | General Security Measures
DHCPv6 Snooping

Command Usage
When the switch receives DHCPv6 packets from clients that already include DHCP Option 37 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCPv6 packets, keep the existing information, or replace it with the switch’s relay agent information.

Example
This example configures the switch to keep existing remote-id option 37 information within DHCPv6 client packets and forward it.

Example
```
Console(config)#ipv6 dhcp snooping option remote-id policy keep
Console(config)#
```

ipv6 dhcp snooping

This command enables DHCPv6 snooping on the specified VLAN. Use the no form to restore the default setting.

Syntax

```
[no] ipv6 dhcp snooping vlan {vlan-id | vlan-range}
```

- `vlan-id` - ID of a configured VLAN (Range: 1-4094)
- `vlan-range` - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
- When DHCPv6 snooping enabled globally using the `ipv6 dhcp snooping` command, and enabled on a VLAN with this command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN as specified by the `ipv6 dhcp snooping trust` command.

- When the DHCPv6 snooping is globally disabled, DHCPv6 snooping can still be configured for specific VLANs, but the changes will not take effect until DHCPv6 snooping is globally re-enabled.

- When DHCPv6 snooping is enabled globally, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.
Example
This example enables DHCP6 snooping for VLAN 1.

```
Console(config)#ipv6 dhcp snooping vlan 1
Console(config)#
```

Related Commands
ipv6 dhcp snooping (310)
ipv6 dhcp snooping trust (315)

**ipv6 dhcp snooping max-binding**
This command sets the maximum number of entries which can be stored in the binding database for an interface. Use the no form to restore the default setting.

**Syntax**

```
ipv6 dhcp snooping max-binding count
no ipv6 dhcp snooping max-binding
```

- **count** - Maximum number of entries. (Range: 1-5)

**Default Setting**
5

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

Example
This example sets the maximum number of binding entries to 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 dhcp snooping max-binding 1
Console(config-if)#
```

**ipv6 dhcp snooping trust**
This command configures the specified interface as trusted. Use the no form to restore the default setting.

**Syntax**

```
[no] ipv6 dhcp snooping trust
```

**Default Setting**
All interfaces are untrusted

**Command Mode**
Interface Configuration (Ethernet, Port Channel)
Chapter 8 | General Security Measures

DHCPv6 Snooping

Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.

- Set all ports connected to DHCPv6 servers within the local network or firewall to trusted, and all other ports outside the local network or firewall to untrusted.

- When DHCPv6 snooping is enabled globally using the `ipv6 dhcp snooping` command, and enabled on a VLAN with `ipv6 dhcp snooping vlan` command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the `no ipv6 dhcp snooping trust` command.

- When an untrusted port is changed to a trusted port, all the dynamic DHCPv6 snooping bindings associated with this port are removed.

- Additional considerations when the switch itself is a DHCPv6 client – The port(s) through which it submits a client request to the DHCPv6 server must be configured as trusted.

Example

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ipv6 dhcp snooping trust
Console(config-if)#
```

Related Commands

- `ipv6 dhcp snooping (310)`
- `ipv6 dhcp snooping vlan (314)`

**clear ipv6 dhcp snooping binding**

This command clears DHCPv6 snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

Syntax

```
clear ipv6 dhcp snooping binding [mac-address ipv6-address]
```

- `mac-address` - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)
- `ipv6-address` - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
**Command Mode**
Privileged Exec

**Example**

```
Console(config)#clear ipv6 dhcp snooping binding 00-12-cf-01-02-03 2001::1
Console(config)#
```

**clear ipv6 dhcp snooping statistics**

This command clears statistical counters for DHCPv6 snooping client, server and relay packets.

**Command Mode**
Privileged Exec

**Example**

```
Console(config)#clear ipv6 dhcp snooping statistics
Console(config)#
```

**show ipv6 dhcp snooping**

This command shows the DHCPv6 snooping configuration settings.

**Command Mode**
Privileged Exec

**Example**

```
Console#show ipv6 dhcp snooping
Global DHCPv6 Snooping status: disabled
DHCPv6 Snooping remote-id option status: disabled
DHCPv6 Snooping remote-id policy: drop
DHCPv6 Snooping is configured on the following VLANs:
  1,

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Max-binding</th>
<th>Current-binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>No</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>No</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/3</td>
<td>No</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/4</td>
<td>No</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/5</td>
<td>Yes</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show ipv6 dhcp snooping binding

This command shows the DHCPv6 snooping binding table entries.

**Command Mode**
Privileged Exec

**Example**

```console
Console#show ipv6 dhcp snooping binding
NA - Non-temporary address
TA - Temporary address

-------------------------------------- ----------- ---- ------- ----
Link-layer Address: 00-13-49-aa-39-26 IPv6 Address                            Lifetime VLAN Port Type
--------------------------------------- ---------- ---- ------- ----
--------------------------------------- ---------- ---- ------- ----
Link-layer Address: 00-12-cf-01-02-03 IPv6 Address                            Lifetime VLAN Port Type
--------------------------------------- ---------- ---- ------- ----
2001:b000::1    2591912    1 Eth 1/3   NA

Console#
```

show ipv6 dhcp snooping statistics

This command shows statistics for DHCPv6 snooping client, server and relay packets.

**Command Mode**
Privileged Exec

**Example**

```console
Console#show ipv6 dhcp snooping statistics
DHCPv6 Snooping Statistics:
Client Packet: Solicit, Request, Confirm, Renew, Rebind,
Decline, Release, Information-request
Server Packet: Advertise, Reply, Reconfigure
Relay Packet: Relay-forward, Relay-reply

State     Client    Server    Relay     Total
--------  --------  --------  --------  --------
Received  10        9         0        19
Sent      9         9         0        18
Dropped   1         0         0        1

Console#
```
IPv4 Source Guard

IPv4 Source Guardv4 is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IPv4 Source Guard table, or dynamic entries in the DHCPv4 Snooping table when enabled (see “DHCPv4 Snooping” on page 296). IPv source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IPv4 Source Guard.

Table 58: IP Source Guard Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip source-guard binding</td>
<td>Adds a static address to the source-guard binding table</td>
<td>GC</td>
</tr>
<tr>
<td>ip source-guard</td>
<td>Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address</td>
<td>IC</td>
</tr>
<tr>
<td>ip source-guard max-binding</td>
<td>Sets the maximum number of entries that can be bound to an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ip source-guard mode</td>
<td>Sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table</td>
<td>IC</td>
</tr>
<tr>
<td>clear ip source-guard binding blocked</td>
<td>Remove all blocked records</td>
<td>IC</td>
</tr>
<tr>
<td>show ip source-guard</td>
<td>Shows whether source guard is enabled or disabled on each interface</td>
<td>PE</td>
</tr>
<tr>
<td>show ip source-guard binding</td>
<td>Shows the source guard binding table</td>
<td>PE</td>
</tr>
</tbody>
</table>

### ip source-guard binding

This command adds a static address to the source-guard ACL or MAC address binding table. Use the **no** form to remove a static entry.

**Syntax**

```
ip source-guard binding [mode {acl | mac}] mac-address
  vlan vlan-id ip-address interface ethernet unit/port-list
no ip source-guard binding [mode {acl | mac}] mac-address vlan vlan-id
```

- **mode** - Specifies the binding mode.
  - **acl** - Adds binding to ACL table.
  - **mac** - Adds binding to MAC address table.

- **mac-address** - A valid unicast MAC address.

- **vlan-id** - ID of a configured VLAN for an ACL filtering table or a range of VLANs for a MAC address filtering table. To specify a list separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094)

- **ip-address** - A valid unicast IP address, including classtful types A, B or C.
unit - Unit identifier. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-28/52)

Default Setting
No configured entries

Command Mode
Global Configuration

Command Usage
◆ If the binding mode is not specified in this command, the entry is bound to the ACL table by default.

◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.

◆ All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ip source-guard command (page 325).

◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.

◆ Static bindings are processed as follows:
  ■ If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.
  ■ If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
  ■ If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Example
This example configures a static source-guard binding on port 5. Since the binding mode is not specified, the entry is bound to the ACL table by default.

```
Console(config)#ip source-guard binding 00-ab-cd-11-22-33 vlan 1 192.168.0.99
interface ethernet 1/5
Console(config-if)#
```
Related Commands
ip source-guard (321)
ip dhcp snooping (297)
ip dhcp snooping vlan (304)

**ip source-guard**  This command configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

**Syntax**

```
ip source-guard {sip | sip-mac}
no ip source-guard
```

- **sip** - Filters traffic based on IP addresses stored in the binding table.
- **sip-mac** - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or firewall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

- Setting source guard mode to "sip" or "sip-mac" enables this function on the selected port. Use the “sip” option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the “sip-mac” option to check these same parameters, plus the source MAC address. Use the **no ip source-guard** command to disable this function on the selected port.

- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier.

- Static addresses entered in the source guard binding table with the **ip source-guard binding** command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.

- If the IP source guard is enabled, an inbound packet’s IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be
checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:
  
  - If DHCPv4 snooping is disabled (see page 297), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  
  - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
  
  - If IP source guard is enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.
  
  - Only unicast addresses are accepted for static bindings.

**Example**

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

**Related Commands**

- `ip source-guard binding (319)`
- `ip dhcp snooping (297)`
- `ip dhcp snooping vlan (304)`
ip source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the no form to restore the default setting.

Syntax

ip source-guard [mode {acl | mac}] max-binding number

no ip source-guard [mode {acl | mac}] max-binding

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL table.

mac - Searches for addresses in the MAC address table.

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-16 for ACL mode; 1-1024 for MAC mode)

Default Setting

5

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by the ip source-guard command.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry. The mode is not specified, and therefore defaults to the ACL binding table.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

clear ip source-guard binding blocked

This command clears source-guard binding table entries from RAM.

Syntax

clear ip source-guard binding blocked

Command Mode

Privileged Exec

Command Usage

When IP Source-Guard detects an invalid packet it creates a blocked record. These records can be viewed using the show ip source-guard
**binding blocked** command. A maximum of 512 blocked records can be stored before the switch overwrites the oldest record with new blocked records. Use the **clear ip source-guard binding blocked** command to clear this table.

**Example**
This command clears the blocked record table.

```console
Console(config)#clear ip source-guard binding blocked
Console(config)#
```

**ip source-guard mode** This command sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table. Use the **no** form to restore the default setting.

**Syntax**

```console
ip source-guard mode {acl | mac}
no ip source-guard mode
```

**mode** - Specifies the learning mode.
- **acl** - Searches for addresses in the ACL binding table.
- **mac** - Searches for addresses in the MAC address binding table.

**Default Setting**
ACL

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**
There are two modes for the filtering table:
- **ACL** - IP traffic will be forwarded if it passes the checking process in the ACL mode binding table.
- **MAC** - A MAC entry will be added in MAC address table if IP traffic passes the checking process in MAC mode binding table.

**Example**
This command sets the binding table mode for the specified interface to MAC mode:

```console
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard mode mac
Console(config-if)#
```
show ip source-guard This command shows whether source guard is enabled or disabled on each interface.

Command Mode
Privileged Exec

Example

```
Console#show ip source-guard

ACL Table | MAC Table
----------|----------
Interface | Filter-type | Filter-table | Max-binding | Max-binding
---------| -----------| ------------| -----------| 1024
Eth 1/1   | DISABLED   | ACL         | 5           | 1024
Eth 1/2   | DISABLED   | ACL         | 5           | 1024
Eth 1/3   | DISABLED   | ACL         | 5           | 1024
Eth 1/4   | DISABLED   | ACL         | 5           | 1024
Eth 1/5   | DISABLED   | ACL         | 5           | 1024
```

show ip source-guard binding This command shows the source guard binding table.

Syntax

```
show ip source-guard binding [dhcp-snooping | static [acl | mac] | blocked [vlan vlan-id | interface interface]
```

- **dhcp-snooping** - Shows dynamic entries configured with DHCP Snooping commands (see page 296)
- **static** - Shows static entries configured with the `ip source-guard binding` command (see page 319).
  - **acl** - Shows static entries in the ACL binding table.
  - **mac** - Shows static entries in the MAC address binding table.
- **blocked** - Shows MAC addresses which have been blocked by IP Source Guard.
  - **vlan-id** - ID of a configured VLAN (Range: 1-4094)
  - **interface** - Specifies a port interface.

Command Mode
Privileged Exec
Chapter 8 | General Security Measures
IPv6 Source Guard

Example

```
Console#show ip source-guard binding
MacAddress        IpAddress       Lease(sec) Type     VLAN Interface
----------------- --------------- ---------- -------------------- ---- --------
11-22-33-44-55-66 192.168.0.99             0 Static                  1 Eth 1/5
Console#
```

IPv6 Source Guard

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled (see “DHCPv6 Snooping” on page 309). IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes commands used to configure IPv6 Source Guard.

Table 59: IPv6 Source Guard Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 source-guard binding</td>
<td>Adds a static address to the source-guard binding table</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 source-guard</td>
<td>Configures the switch to filter inbound traffic based on source IP address</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 source-guard max-</td>
<td>Sets the maximum number of entries that can be bound to an interface</td>
<td>IC</td>
</tr>
<tr>
<td>binding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ipv6 source-guard</td>
<td>Shows whether source guard is enabled or disabled on each interface</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 source-guard binding</td>
<td>Shows the source guard binding table</td>
<td>PE</td>
</tr>
</tbody>
</table>

**ipv6 source-guard binding**

This command adds a static address to the source-guard binding table. Use the no form to remove a static entry.

**Syntax**

```
ipv6 source-guard binding mac-address vlan vlan-id ipv6-address interface interface

no ipv6 source-guard binding mac-address vlan vlan-id
```

- `mac-address` - A valid unicast MAC address.
- `vlan-id` - ID of a configured VLAN (Range: 1-4094)
- `ipv6-address` - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
interface

**ethernet unit/port**

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-28/52)

**Default Setting**
No configured entries

**Command Mode**
Global Configuration

**Command Usage**
- Table entries include an associated MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Snooping, Dynamic-DHCPv6-Snooping), VLAN identifier, and port identifier.
- Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.
- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the `show ipv6 source-guard` command.
- When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 snooping, or static addresses configured in the source guard binding table with this command.
- Static bindings are processed as follows:
  - If there is no entry with same MAC address and IPv6 address, a new entry is added to binding table using static IPv6 source guard binding.
  - If there is an entry with same MAC address and IPv6 address, and the type of entry is static IPv6 source guard binding, then the new entry will replace the old one.
  - If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IPv6 source guard binding.
  - Only unicast addresses are accepted for static bindings.
Example
This example configures a static source-guard binding on port 5.

```
Console(config)#ipv6 source-guard binding 00-ab-11-cd-23-45 vlan 1 2001::1
   interface ethernet 1/5
Console(config)#
```

Related Commands
ipv6 source-guard (328)
ipv6 dhcp snooping (310)
ipv6 dhcp snooping vlan (314)

**ipv6 source-guard** This command configures the switch to filter inbound traffic based on the source IP address stored in the binding table. Use the no form to disable this function.

**Syntax**
```
ipv6 source-guard sip
no ipv6 source-guard
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**
◆ Source guard is used to filter traffic on an insecure port which receives messages from outside the network or firewall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

◆ This command checks the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table. Use the no ipv6 source guard command to disable this function on the selected port.

◆ After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.

◆ Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Snooping, Dynamic-DHCPv6-Snooping), VLAN identifier, and port identifier.
Static addresses entered in the source guard binding table with the `ipv6 source-guard binding` command are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.

If IPv6 source guard is enabled, an inbound packet’s source IPv6 address will be checked against the binding table. If no matching entry is found, the packet will be dropped.

Filtering rules are implemented as follows:
- If ND snooping and DHCPv6 snooping are disabled, IPv6 source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, the packet will be forwarded.
- If ND snooping or DHCPv6 snooping is enabled, IPv6 source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.
- If IPv6 source guard if enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCPv6 snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets.
- Only IPv6 global unicast addresses are accepted for static bindings.

**Example**
This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard sip
Console(config-if)#
```

**RELATED COMMANDS**
- `ipv6 source-guard binding` (326)
- `ipv6 dhcp snooping` (310)
- `ipv6 dhcp snooping vlan` (314)

**ipv6 source-guard max-binding**
This command sets the maximum number of entries that can be bound to an interface. Use the `no` form to restore the default setting.

**Syntax**
```
ipv6 source-guard max-binding number

no ipv6 source-guard max-binding
```

`number` - The maximum number of IPv6 addresses that can be mapped to an interface in the binding table. (Range: 1-5)
**Default Setting**
5

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**
◆ This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping, and static entries set by the `ipv6 source-guard` command.

◆ IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.

◆ If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by the `ipv6 source-guard max-binding` command. In other words, no new entries will be added to the IPv6 source guard binding table.

◆ If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

**Example**
This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard max-binding 1
Console(config-if)#
```

**show ipv6 source-guard**
This command shows whether IPv6 source guard is enabled or disabled on each interface, and the maximum allowed bindings.

**Command Mode**
Privileged Exec

**Example**

```
Console#show ipv6 source-guard
+---------+------------+----------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Max-binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>DISABLED</td>
<td>5</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>DISABLED</td>
<td>5</td>
</tr>
</tbody>
</table>
```

- 330 -
**Chapter 8 | General Security Measures**

**ARP Inspection**

<table>
<thead>
<tr>
<th>Eth 1/3</th>
<th>DISABLED</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/4</td>
<td>DISABLED</td>
<td>5</td>
</tr>
<tr>
<td>Eth 1/5</td>
<td>SIP</td>
<td>1</td>
</tr>
<tr>
<td>Eth 1/6</td>
<td>DISABLED</td>
<td>5</td>
</tr>
</tbody>
</table>

**show ipv6 source-guard binding**

This command shows the IPv6 source guard binding table.

**Syntax**

```
show ipv6 source-guard binding [dynamic | static]
```

- **dynamic** - Shows dynamic entries configured with ND Snooping or DHCPv6 Snooping commands (see page 309)
- **static** - Shows static entries configured with the `ipv6 source-guard binding` command.

**Command Mode**

Privileged Exec

**Example**

```
Console#show ipv6 source-guard binding
MAC Address    IPv6 Address                            VLAN Interface Type
-------------- --------------------------------------- ---- --------- ----
00AB-11CD-2345                                 2001::1    1  Eth 1/5   STA
```

**ARP Inspection**

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.
This section describes commands used to configure ARP Inspection.

Table 60: ARP Inspection Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp inspection</td>
<td>Enables ARP Inspection globally on the switch</td>
<td>GC</td>
</tr>
<tr>
<td>ip arp inspection filter</td>
<td>Specifies an ARP ACL to apply to one or more VLANs</td>
<td>GC</td>
</tr>
<tr>
<td>ip arp inspection log-buffer logs</td>
<td>Sets the maximum number of entries saved in a log message, and the rate at these messages are sent</td>
<td>GC</td>
</tr>
<tr>
<td>ip arp inspection validate</td>
<td>Specifies additional validation of address components in an ARP packet</td>
<td>GC</td>
</tr>
<tr>
<td>ip arp inspection vlan</td>
<td>Enables ARP Inspection for a specified VLAN or range of VLANs</td>
<td>GC</td>
</tr>
<tr>
<td>ip arp inspection limit</td>
<td>Sets a rate limit for the ARP packets received on a port</td>
<td>IC</td>
</tr>
<tr>
<td>ip arp inspection trust</td>
<td>Sets a port as trusted, and thus exempted from ARP Inspection</td>
<td>IC</td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Displays the global configuration settings for ARP Inspection</td>
<td>PE</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Shows the trust status and inspection rate limit for ports</td>
<td>PE</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Shows information about entries stored in the log, including the associated VLAN, port, and address components</td>
<td>PE</td>
</tr>
<tr>
<td>log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Shows statistics about the number of ARP packets processed, or dropped for various reasons</td>
<td>PE</td>
</tr>
<tr>
<td>statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Shows configuration setting for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ACL validation is completed</td>
<td>PE</td>
</tr>
<tr>
<td>vlan</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ip arp inspection

This command enables ARP Inspection globally on the switch. Use the no form to disable this function.

**Syntax**

```
[no] ip arp inspection
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the `ip arp inspection vlan` command.
◆ When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.

◆ When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.

◆ When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.

◆ Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.

◆ When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

```
Console(config)#ip arp inspection
Console(config)#
```

**ip arp inspection filter**

This command specifies an ARP ACL to apply to one or more VLANs. Use the **no** form to remove an ACL binding. Use the **no** form to remove an ACL binding.

**Syntax**

```
ip arp inspection filter arp-acl-name vlan {vlan-id | vlan-range} [static]
no ip arp inspection filter arp-acl-name vlan {vlan-id | vlan-range}
```

- **arp-acl-name** - Name of an ARP ACL. (Maximum length: 16 characters)
- **vlan-id** - VLAN ID. (Range: 1-4094)
- **vlan-range** - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.
- **static** - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

**Default Setting**

ARP ACLs are not bound to any VLAN
Static mode is not enabled

**Command Mode**

Global Configuration
Command Usage
◆ ARP ACL configuration commands are described under “ARP ACLs” on page 370.

◆ If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.

◆ If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

Example

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

**ip arp inspection log-buffer logs**

This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the no form to restore the default settings.

Syntax

```
ip arp inspection log-buffer logs message-number interval seconds
no ip arp inspection log-buffer logs
```

- **message-number** - The maximum number of entries saved in a log message. (Range: 0-256, where 0 means no events are saved and no messages sent)
- **seconds** - The interval at which log messages are sent. (Range: 0-86400)

Default Setting
Message Number: 5
Interval: 1 second

Command Mode
Global Configuration

Command Usage
◆ ARP Inspection must be enabled with the ip arp inspection command before this command will be accepted by the switch.

◆ By default, logging is active for ARP Inspection, and cannot be disabled.

◆ When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
◆ If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.

◆ The maximum number of entries that can be stored in the log buffer is determined by the `message-number` parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.

◆ The switch generates a system message on a rate-controlled basis determined by the `seconds` values. After the system message is generated, all entries are cleared from the log buffer.

**Example**

```plaintext
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

**ip arp inspection validate** This command specifies additional validation of address components in an ARP packet. Use the `no` form to restore the default setting.

**Syntax**

```
ip arp inspection validate
   {dst-mac [ip [allow-zeros] [src-mac]] | ip [allow-zeros] [src-mac]] | src-mac}
```

**no ip arp inspection validate**

`dst-mac` - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

`ip` - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

`allow-zeros` - Allows sender IP address to be 0.0.0.0.

`src-mac` - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

**Default Setting**
No additional validation is performed

**Command Mode**
Global Configuration
**Command Usage**
By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

**Example**

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

**ip arp inspection vlan**
This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

**Syntax**

```
[no] ip arp inspection vlan {vlan-id | vlan-range}
```

- `vlan-id` - VLAN ID. (Range: 1-4094)
- `vlan-range` - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

**Default Setting**
Disabled on all VLANs

**Command Mode**
Global Configuration

**Command Usage**

- When ARP Inspection is enabled globally with the `ip arp inspection` command, it becomes active only on those VLANs where it has been enabled with this command.

- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.

- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.

- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.

- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.

- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.
**Example**

```console
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

**ip arp inspection limit**  This command sets a rate limit for the ARP packets received on a port. Use the no form to restore the default setting.

**Syntax**

```
ip arp inspection limit {rate pps | none}
```

```
no ip arp inspection limit
```

- **rate pps** - The maximum number of ARP packets that can be processed by the CPU per second on trusted or untrusted ports. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)
- **none** - There is no limit on the number of ARP packets that can be processed by the CPU.

**Default Setting**

15

**Command Mode**

Interface Configuration (Port, Static Aggregation)

**Command Usage**

- This command applies to both trusted and untrusted ports.
- When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

**ip arp inspection trust**  This command sets a port as trusted, and thus exempted from ARP Inspection. Use the no form to restore the default setting.

**Syntax**

```
[no] ip arp inspection trust
```

**Default Setting**

Untrusted
Command Mode
Interface Configuration (Port, Static Aggregation)

Command Usage
Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

Example
```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration
This command displays the global configuration settings for ARP Inspection.

Command Mode
Privileged Exec

Example
```
Console#show ip arp inspection configuration

ARP inspection global information:

  Global IP ARP Inspection status : disabled
  Log Message Interval : 10 s
  Log Message Number : 1
  Need Additional Validation(s) : Yes
  Additional Validation Type : Destination MAC address

Console#
```

show ip arp inspection interface
This command shows the trust status and ARP Inspection rate limit for ports.

Syntax
```
show ip arp inspection interface [interface]

interface

  ethernet unit/port

    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)
```

Command Mode
Privileged Exec
Example

```
Console#show ip arp inspection interface ethernet 1/1
Port Number            Trust Status             Rate Limit (pps)
-------------   --------------------    ------------------------------
Eth 1/1            trusted                    150

Console#
```

**show ip arp inspection log** This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

**Command Mode**
Privileged Exec

Example

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port  Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- --- ---- --------------  --------------  ---------------  --------------
1   1     11  192.168.2.2     192.168.2.1     00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF

Console#
```

**show ip arp inspection statistics** This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

**Command Mode**
Privileged Exec

Example

```
Console#show ip arp inspection statistics
ARP packets received before rate limit : 150
ARP packets dropped due to rate limit : 5
Total ARP packets processed by ARP Inspection : 150
ARP packets dropped by additional validation (source MAC address) : 0
ARP packets dropped by additional validation (destination MAC address) : 0
ARP packets dropped by additional validation (IP address) : 0
ARP packets dropped by ARP ACLs : 0
ARP packets dropped by DHCP snooping : 0

Console#
```
**show ip arp inspection vlan**

This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

**Syntax**

```
show ip arp inspection vlan [vlan-id | vlan-range]
```

- **vlan-id** - VLAN ID. (Range: 1-4094)
- **vlan-range** - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

**Command Mode**

Privileged Exec

**Example**

```
Console#show ip arp inspection vlan 1

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>DAi Status</th>
<th>ACL Name</th>
<th>ACL Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>disabled</td>
<td>sales</td>
<td>static</td>
</tr>
</tbody>
</table>

Console#
```

---

**Denial of Service Protection**

A denial-of-service attack (DoS attack) is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately.

This section describes commands used to protect against DoS attacks.

**Table 61: DoS Protection Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos-protection echo-chargen</td>
<td>Protects against DoS echo/chargen attacks</td>
<td>GC</td>
</tr>
<tr>
<td>dos-protection smurf</td>
<td>Protects against DoS smurf attacks</td>
<td>GC</td>
</tr>
<tr>
<td>dos-protection tcp-flooding</td>
<td>Protects against DoS TCP-flooding attacks</td>
<td>GC</td>
</tr>
<tr>
<td>dos-protection tcp-null-scan</td>
<td>Protects against DoS TCP-null-scan attacks</td>
<td>GC</td>
</tr>
<tr>
<td>dos-protection tcp-syn-fin-scan</td>
<td>Protects against DoS TCP-SYN/FIN-scan attacks</td>
<td>GC</td>
</tr>
<tr>
<td>dos-protection tcp-udp-port-zero</td>
<td>Protects against attacks which set the Layer 4 source or destination port to zero</td>
<td>GC</td>
</tr>
<tr>
<td>dos-protection tcp-xmas-scan</td>
<td>Protects against DoS TCP-XMAS-scan attacks</td>
<td>GC</td>
</tr>
</tbody>
</table>
This command protects against DoS echo/chargen attacks in which the echo service repeats anything sent to it, and the chargen (character generator) service generates a continuous stream of data. When used together, they create an infinite loop and result in a denial-of-service. Use the `no` form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

**Syntax**

```
  dos-protection echo-chargen [bit-rate-in-kilo rate]
  no dos-protection echo-chargen [bit-rate-in-kilo rate]
```

*rate* – Maximum allowed rate. (Range: 64-2000 kbits/second)

**Default Setting**

Disabled, 1000 kbits/second

**Command Mode**

Global Configuration

**Example**

```
Console(config)#dos-protection echo-chargen bit-rate-in-kilo 65
Console(config)#
```

dos-protection smurf

This command protects against DoS smurf attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should crash due to the many interrupts required to send ICMP Echo response packets. Use the `no` form to disable this feature.

**Syntax**

```
  [no] dos-protection smurf
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration
Denial of Service Protection

Example

```console
Console(config)#dos-protection smurf
Console(config)#
```

dos-protection tcp-flooding

This command protects against DoS TCP-flooding attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. Use the no form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

Syntax

```
dos-protection tcp-flooding [bit-rate-in-kilo rate]
no dos-protection tcp-flooding [bit-rate-in-kilo rate]
```

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Setting

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

```console
Console(config)#dos-protection tcp-flooding bit-rate-in-kilo 65
Console(config)#
```

dos-protection tcp-null-scan

This command protects against DoS TCP-null-scan attacks in which a TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target’s TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. Use the no form to disable this feature.

Syntax

```
[no] dos-protection tcp-null-scan
```

Default Setting

Enabled

Command Mode

Global Configuration
**Example**

```
Console(config)#dos-protection tcp-null-scan
Console(config)#
```

**dos-protection tcp-syn-fin-scan**

This command protects against DoS TCP-SYN/FIN-scan attacks in which a TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. Use the **no** form to disable this feature.

**Syntax**

```
[no] dos-protection tcp-syn-fin-scan
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Example**

```
Console(config)#dos-protection tcp-syn-fin-scan
Console(config)#
```

**dos-protection tcp-udp-port-zero**

This command protects against DoS attacks in which the TCP or UDP source port or destination port is set to zero. This technique may be used as a form of DoS attack, or it may just indicate a problem with the source device. When this command is enabled, the switch will drop these packets. Use the **no** form to restore the default setting.

**Syntax**

```
[no] dos-protection tcp-udp-port-zero
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Example**

```
Console(config)#dos-protection tcp-udp-port-zero
Console(config)#
```
**dos-protection tcp-xmas-scan**
This command protects against DoS TCP-xmas-scan in which a so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target’s TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. Use the *no* form to disable this feature.

**Syntax**

```
[no] dos-protection tcp-xmas-scan
```

**Default Setting**
Enabled

**Command Mode**
Global Configuration

**Example**

```
Console(config)#dos-protection tcp-xmas-scan
Console(config)#
```

---

**dos-protection udp-flooding**
This command protects against DoS UDP-flooding attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. Use the *no* form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

**Syntax**

```
dos-protection udp-flooding [bit-rate-in-kilo rate]
no dos-protection udp-flooding [bit-rate-in-kilo rate]
```

*rate* – Maximum allowed rate. (Range: 64-2000 kbits/second)

**Default Setting**
Disabled, 1000 kbits/second

**Command Mode**
Global Configuration

**Example**

```
Console(config)#dos-protection udp-flooding bit-rate-in-kilo 65
Console(config)#
```
**dos-protection win-nuke**  This command protects against DoS WinNuke attacks in which affected the Microsoft Windows 3.1x/95/NT operating systems. In this type of attack, the perpetrator sends the string of OOB out-of-band (OOB) packets contained a TCP URG flag to the target computer on TCP port 139 (NetBIOS), casing it to lock up and display a “Blue Screen of Death.” This did not cause any damage to, or change data on, the computer’s hard disk, but any unsaved data would be lost. Microsoft made patches to prevent the WinNuke attack, but the OOB packets still put the service in a tight loop that consumed all available CPU time. Use the no form without the bit rate parameter to disable this feature, or with the bit rate parameter to restore the default rate limit.

**Syntax**

```
dos-protection win-nuke [bit-rate-in-kilo rate]
```

```
no dos-protection udp-flooding [bit-rate-in-kilo rate]
```

`rate` – Maximum allowed rate. (Range: 64-2000 kbits/second)

**Default Setting**

Disabled, 1000 kbits/second

**Command Mode**

Global Configuration

**Example**

```
Console(config)#dos-protection win-nuke bit-rate-in-kilo 65
Console(config)#
```

**show dos-protection**  This command shows the configuration settings for the DoS protection commands.

**Command Mode**

Privileged Exec

**Example**

```
Console#show dos-protection
Global DoS Protection:

  Echo/Chargen Attack : Disabled, 1000 kilobits per second
  Smurf Attack        : Enabled
  TCP Flooding Attack : Disabled, 1000 kilobits per second
  TCP Null Scan       : Enabled
  TCP SYN/FIN Scan    : Enabled
  TCP/UDP Packets with Port 0 : Enabled
  TCP XMAS Scan       : Enabled
  UDP Flooding Attack : Disabled, 1000 kilobits per second
  WinNuke Attack      : Disabled, 1000 kilobits per second

Console#
```
Port-based Traffic Segmentation

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client’s allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

<table>
<thead>
<tr>
<th>Table 62: Commands for Configuring Traffic Segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>traffic-segmentation</td>
</tr>
<tr>
<td>traffic-segmentation session</td>
</tr>
<tr>
<td>traffic-segmentation uplink/downlink</td>
</tr>
<tr>
<td>traffic-segmentation uplink-to-uplink</td>
</tr>
<tr>
<td>show traffic-segmentation</td>
</tr>
</tbody>
</table>

**traffic-segmentation** This command enables traffic segmentation. Use the **no** form to disable traffic segmentation.

**Syntax**

```
[no] traffic-segmentation
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

◆ Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.

◆ Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.
When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 63: Traffic Segmentation Forwarding

<table>
<thead>
<tr>
<th>Destination Source</th>
<th>Session #1 Downlinks</th>
<th>Session #1 Uplinks</th>
<th>Session #2 Downlinks</th>
<th>Session #2 Uplinks</th>
<th>Normal Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session #1 Downlink Ports</td>
<td>Blocking</td>
<td>Forwarding</td>
<td>Blocking</td>
<td>Blocking</td>
<td>Blocking</td>
</tr>
<tr>
<td>Session #1 Uplink Ports</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Blocking</td>
<td>Blocking/Forwarding*</td>
<td>Forwarding</td>
</tr>
<tr>
<td>Session #2 Downlink Ports</td>
<td>Blocking</td>
<td>Blocking</td>
<td>Blocking</td>
<td>Forwarding</td>
<td>Blocking</td>
</tr>
<tr>
<td>Session #2 Uplink Ports</td>
<td>Blocking</td>
<td>Blocking/Forwarding*</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Forwarding</td>
</tr>
<tr>
<td>Normal Ports</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>

* The forwarding state for uplink-to-uplink ports is configured by the traffic-segmentation uplink-to-uplink command.

When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.

Enter the traffic-segmentation command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the traffic-segmentation uplink/downlink command.

Enter no traffic-segmentation to disable traffic segmentation and clear the configuration settings for segmented groups.

Example

This example enables traffic segmentation globally on the switch.

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session

This command creates a traffic-segmentation client session. Use the no form to remove a client session.

Syntax

```
[no] pvlan session session-id
```

session-id – Traffic segmentation session. (Range: 1-4)

Default Setting

None
**Command Mode**
Global Configuration

**Command Usage**
- Use this command to create a new traffic-segmentation client session.

- Using the no form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

**Example**

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

**traffic-segmentation uplink/downlink**

This command configures the uplink and down-link ports for a segmented group of ports. Use the no form to remove a port from the segmented group.

**Syntax**

```
[no] traffic-segmentation [session session-id] [uplink interface-list]
[downlink interface-list] | downlink interface-list

session-id – Traffic segmentation session. (Range: 1-4)
uplink – Specifies an uplink interface.
downlink – Specifies a downlink interface.
interface

  ethernet unit/port
  unit - Unit identifier. (Range: 1)
  port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)
```

**Default Setting**
Session 1 if not defined
No segmented port groups are defined.

**Command Mode**
Global Configuration

**Command Usage**
- A port cannot be configured in both an uplink and downlink list.

- A port can only be assigned to one traffic-segmentation session.

- When specifying an uplink or downlink, a list of ports may be entered by using a hyphen or comma in the port field. Note that lists are not supported for the channel-id field.
A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.

If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

**Example**
This example enables traffic segmentation, and then sets port 10 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
downlink ethernet 1/5-8
Console(config)#
```

**traffic-segmentation**
This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the `no` form to restore the default.

**Syntax**
```
[no] traffic-segmentation uplink-to-uplink {blocking | forwarding}
```
- **blocking** – Blocks traffic between uplink ports assigned to different sessions.
- **forwarding** – Forwards traffic between uplink ports assigned to different sessions.

**Default Setting**
Blocking

**Command Mode**
Global Configuration

**Example**
This example enables forwarding of traffic between uplink ports assigned to different client sessions.

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```
show traffic-segmentation

This command displays the configured traffic segments.

**Command Mode**
Privileged Exec

**Example**

```
Console#show traffic-segmentation

Private VLAN Status : Enabled
Uplink-to-Uplink Mode : Forwarding

+-----------+-----------------+-----------------+
<table>
<thead>
<tr>
<th>Session</th>
<th>Uplink Ports</th>
<th>Downlink Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet 1/1</td>
<td>Ethernet 1/2</td>
</tr>
<tr>
<td></td>
<td>Ethernet 1/3</td>
<td>Ethernet 1/3</td>
</tr>
<tr>
<td></td>
<td>Ethernet 1/4</td>
<td>Ethernet 1/4</td>
</tr>
</tbody>
</table>

Console#
```
Access Control Lists

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, next header type, or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

**Table 64: Access Control List Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 ACLs</td>
<td>Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code</td>
</tr>
<tr>
<td>IPv6 ACLs</td>
<td>Configures ACLs based on IPv6 addresses, DSCP traffic class, or next header type</td>
</tr>
<tr>
<td>MAC ACLs</td>
<td>Configures ACLs based on hardware addresses, packet format, and Ethernet type</td>
</tr>
<tr>
<td>ARP ACLs</td>
<td>Configures ACLs based on ARP messages addresses</td>
</tr>
<tr>
<td>ACL Information</td>
<td>Displays ACLs and associated rules; shows ACLs assigned to each port</td>
</tr>
</tbody>
</table>

**IPv4 ACLs**

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

**Table 65: IPv4 ACL Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list ip</td>
<td>Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs</td>
<td>GC</td>
</tr>
<tr>
<td>permit, deny</td>
<td>Filters packets matching a specified source IPv4 address</td>
<td>IPv4-STD-ACL</td>
</tr>
<tr>
<td>permit, deny</td>
<td>Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code</td>
<td>IPv4-EXT-ACL</td>
</tr>
<tr>
<td>ip access-group</td>
<td>Binds an IPv4 ACL to a port</td>
<td>IC</td>
</tr>
<tr>
<td>show ip access-group</td>
<td>Shows port assignments for IPv4 ACLs</td>
<td>PE</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the rules for configured IPv4 ACLs</td>
<td>PE</td>
</tr>
</tbody>
</table>
**access-list ip**  This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the *no* form to remove the specified ACL.

**Syntax**

```plaintext
[no] access-list ip {standard | extended} acl-name
```

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- **acl-name** – Name of the ACL. (Maximum length: 32 characters)

**Default Setting**
None

**Command Mode**
Global Configuration

**Command Usage**
- When you create a new ACL or enter configuration mode for an existing ACL, use the *permit* or *deny* command to add new rules to the bottom of the list.
- To remove a rule, use the *no permit* or *no deny* command followed by the exact text of a previously configured rule.
- An ACL can contain up to 128 rules.

**Example**

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

**Related Commands**
- *permit*, *deny*, *redirect-to* (353)
- *ip access-group* (356)
- *show ip access-list* (357)
**permit, deny**  
*(Standard IP ACL)*  
This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

**Syntax**

```
{permit | deny}
{any | source bitmask | host source}
[time-range time-range-name]
```

**no {permit | deny}
{any | source bitmask | host source}

- **any** – Any source IP address.
- **source** – Source IP address.
- **bitmask** – Dotted decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- **time-range-name** - Name of the time range. (Range: 1-32 characters)

**Default Setting**
None

**Command Mode**
Standard IPv4 ACL

**Command Usage**

- New rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

**Example**

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
```

**Related Commands**

- `access-list ip (352)`
- `Time Range (155)`
**permit, deny**  
(Extended IPv4 ACL)  
This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

**Syntax**

```
{permit | deny} [protocol-number | udp]  
{any | source address-bitmask | host source}  
{any | destination address-bitmask | host destination}  
[precedence precedence] [dscp dscp]  
[source-port sport [bitmask]]  
[destination-port dport [port-bitmask]]  
[time-range time-range-name]
```

```
no {permit | deny} [protocol-number | udp]  
{any | source address-bitmask | host source}  
{any | destination address-bitmask | host destination}  
[precedence precedence] [dscp dscp]  
[source-port sport [bitmask]]  
[destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp  
{any | source address-bitmask | host source}  
{any | destination address-bitmask | host destination}  
[precedence precedence] [dscp dscp]  
[source-port sport [bitmask]]  
[destination-port dport [port-bitmask]]  
[control-flag control-flags flag-bitmask]  
[time-range time-range-name]
```

```
no {permit | deny} tcp  
{any | source address-bitmask | host source}  
{any | destination address-bitmask | host destination}  
[precedence precedence] [dscp dscp]  
[source-port sport [bitmask]]  
[destination-port dport [port-bitmask]]  
[control-flag control-flags flag-bitmask]
```

*protocol-number* – A specific protocol number. (Range: 0-255)

*source* – Source IP address.

*destination* – Destination IP address.

*address-bitmask* – Decimal number representing the address bits to match.

*host* – Keyword followed by a specific IP address.

*precedence* – IP precedence level. (Range: 0-7)

*dscp* – DSCP priority level. (Range: 0-63)

*port* – Protocol 4 source port number. (Range: 0-65535)

*dport* – Protocol 4 destination port number. (Range: 0-65535)

---

4. Includes TCP, UDP or other protocol types.
**port-bitmask** – Decimal number representing the port bits to match. (Range: 0-65535)

**control-flags** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

**flag-bitmask** – Decimal number representing the code bits to match.

**time-range-name** - Name of the time range. (Range: 1-32 characters)

**Default Setting**
None

**Command Mode**
Extended IPv4 ACL

**Command Usage**
◆ All new rules are appended to the end of the list.

◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

◆ You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.

◆ The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:

  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

  - SYN flag valid, use “control-code 2 2”
  - Both SYN and ACK valid, use “control-code 18 18”
  - SYN valid and ACK invalid, use “control-code 2 18”
**Example**

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port 80
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-flag 2 2
```

**Related Commands**

access-list ip (352)  
Time Range (155)

**ip access-group**  This command binds an IPv4 ACL to a port. Use the `no` form to remove the port.

**Syntax**

```
ip access-group acl-name in [time-range time-range-name] [counter]
no ip access-group acl-name in
```

- `acl-name` – Name of the ACL. (Maximum length: 32 characters)
- `in` – Indicates that this list applies to ingress packets.
- `time-range-name` - Name of the time range. (Range: 1-32 characters)
- `counter` – Enables counter for ACL statistics.

**Default Setting**

None

**Command Mode**

Interface Configuration (Ethernet)
**Chapter 9 | Access Control Lists**

**IPv4 ACLs**

---

**Command Usage**

- Only one ACL can be bound to a port.

- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

**Example**

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

**Related Commands**

- `show ip access-list` (357)
- `Time Range` (155)

---

**Command Mode**

Privileged Exec

---

**Show ip access-group**

This command shows the ports assigned to IP ACLs.

**Command Mode**

Privileged Exec

**Example**

```
Console#show ip access-group
Interface ethernet 1/2
  IP access-list david in
Console#
```

**Related Commands**

- `ip access-group` (356)

---

**Show ip access-list**

This command displays the rules for configured IPv4 ACLs.

**Syntax**

```
show ip access-list {standard | extended} [acl-name]
```

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- **acl-name** – Name of the ACL. (Maximum length: 32 characters)

**Command Mode**

Privileged Exec
Example

```
Console#show ip access-list standard
IP standard access-list david:
   permit host 10.1.1.21
   permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands

- permit, deny, redirect-to (353)
- ip access-group (356)

IPv6 ACLs

The commands in this section configure ACLs based on IPv6 addresses, DSCP traffic class, or next header type. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 66: IPv6 ACL Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list ipv6</td>
<td>Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs</td>
<td>GC</td>
</tr>
<tr>
<td>permit, deny, redirect to</td>
<td>Filters packets matching a specified source IPv6 address</td>
<td>IPv6-STD-ACL</td>
</tr>
<tr>
<td>permit, deny, redirect to</td>
<td>Filters packets meeting the specified criteria, including destination IPv6 address, DSCP traffic class, or next header type</td>
<td>IPv6-EXT-ACL</td>
</tr>
<tr>
<td>ipv6 access-group</td>
<td>Adds a port to an IPv6 ACL</td>
<td>IC</td>
</tr>
<tr>
<td>show ipv6 access-group</td>
<td>Shows port assignments for IPv6 ACLs</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>Displays the rules for configured IPv6 ACLs</td>
<td>PE</td>
</tr>
</tbody>
</table>

**access-list ipv6**  
This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

**Syntax**

```
[no] access-list ipv6 {standard | extended} acl-name
```

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.
- **acl-name** – Name of the ACL. (Maximum length: 32 characters)
Default Setting
None

Command Mode
Global Configuration

Command Usage

◆ When you create a new ACL or enter configuration mode for an existing ACL, use the `permit` or `deny` command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.

◆ To remove a rule, use the `no permit` or `no deny` command followed by the exact text of a previously configured rule.

◆ An ACL can contain up to 64 rules.

Example

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

Related Commands

`permit`, `deny` (Standard IPv6 ACL) (359)
`permit`, `deny` (Extended IPv6 ACL) (360)
`ipv6 access-group` (362)
`show ipv6 access-list` (363)

**permit, deny** (Standard IPv6 ACL)  This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the `no` form to remove a rule.

Syntax

```
{permit | deny}
{any | host} source-ipv6-address | source-ipv6-address/prefix-length
[time-range time-range-name]

no {permit | deny} {any | host} source-ipv6-address | source-ipv6-address/prefix-length
```

- **any** – Any source IP address.
- **host** – Keyword followed by a specific IP address.
- **source-ipv6-address** - An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

time-range-name - Name of the time range. (Range: 1-32 characters)

Default Setting
None

Command Mode
Standard IPv6 ACL

Command Usage
New rules are appended to the end of the list.

Example
This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

Related Commands
access-list ipv6 (358)
Time Range (155)

permit, deny
(Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, or next header type. Use the no form to remove a rule.

Syntax

```
{permit | deny} {any | host source-ipv6-address | source-ipv6-address[/prefix-length]} {any | destination-ipv6-address/prefix-length} [dscp dscp] [next-header next-header] [time-range time-range-name]
```

```
no {permit | deny} {any | host source-ipv6-address | source-ipv6-address[/prefix-length]} {any | destination-ipv6-address/prefix-length} [dscp dscp] [next-header next-header]
```

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific source IP address.

source-ipv6-address – An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,”
using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 64 bits of the destination address.)

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 for source prefix, 0-8 for destination prefix)

dscp – DSCP traffic class. (Range: 0-63)

next-header – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

time-range-name - Name of the time range. (Range: 1-32 characters)

Default Setting
None

Command Mode
Extended IPv6 ACL

Command Usage
◆ All new rules are appended to the end of the list.

◆ Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

0 : Hop-by-Hop Options (RFC 2460)
6 : TCP Upper-layer Header (RFC 1700)
17 : UDP Upper-layer Header (RFC 1700)
43 : Routing (RFC 2460)
44 : Fragment (RFC 2460)
51 : Authentication (RFC 2402)
50 : Encapsulating Security Payload (RFC 2406)
60 : Destination Options (RFC 2460)

Example
This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the next header is 43.*

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 next-header 43
Console(config-ext-ipv6-acl)#
```

**Related Commands**

*access-list ipv6 (358)*

*Time Range (155)*

**ipv6 access-group** This command binds a port to an IPv6 ACL. Use the *no* form to remove the port.

**Syntax**

```
ipv6 access-group acl-name in [time-range time-range-name] [counter]
no ipv6 access-group acl-name in
```

- **acl-name** – Name of the ACL. (Maximum length: 32 characters)
- **in** – Indicates that this list applies to ingress packets.
- **time-range-name** - Name of the time range. (Range: 1-32 characters)
- **counter** – Enables counter for ACL statistics.

**Default Setting**

None

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- IPv6 ACLs can only be applied to ingress packets.
Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

Related Commands

- `show ipv6 access-list` (363)
- `Time Range` (155)

**show ipv6 access-group**

This command shows the ports assigned to IPv6 ACLs.

**Command Mode**

Privileged Exec

**Example**

```
Console#show ipv6 access-group
Interface ethernet 1/2
IPv6 standard access-list david in
Console#
```

Related Commands

- `ipv6 access-group` (362)

**show ipv6 access-list**

This command displays the rules for configured IPv6 ACLs.

**Syntax**

```
show ipv6 access-list {standard | extended} [acl-name]
```

- `standard` – Specifies a standard IPv6 ACL.
- `extended` – Specifies an extended IPv6 ACL.
- `acl-name` – Name of the ACL. (Maximum length: 32 characters)

**Command Mode**

Privileged Exec

**Example**

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
   permit host 2009:DB9:2229::79
   permit 2009:DB9:2229:5::/64
Console#
```
MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. The ACLs can further specify optional IP and IPv6 addresses including protocol type and upper layer ports. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 67: MAC ACL Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list mac</td>
<td>Creates a MAC ACL and enters configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>permit, deny, redirect-to</td>
<td>Filters packets matching a specified source and destination address, packet format, and Ethernet type. They can be further specified using optional IP and IPv6 addresses including protocol type and upper layer ports.</td>
<td>MAC-ACL</td>
</tr>
<tr>
<td>mac access-group</td>
<td>Binds a MAC ACL to a port</td>
<td>IC</td>
</tr>
<tr>
<td>show mac access-group</td>
<td>Shows port assignments for MAC ACLs</td>
<td>PE</td>
</tr>
<tr>
<td>show mac access-list</td>
<td>Displays the rules for configured MAC ACLs</td>
<td>PE</td>
</tr>
</tbody>
</table>

access-list mac

This command enters MAC ACL configuration mode. Rules can be added to filter packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Rules can also be used to filter packets based on IPv4/IPv6 addresses, including Layer 4 ports and protocol types. Use the no form to remove the specified ACL.

Syntax

[no] access-list mac acl-name

acl-name – Name of the ACL. (Maximum length: 32 characters)

Default Setting
None

Command Mode
Global Configuration

Command Usage
- When you create a new ACL or enter configuration mode for an existing ACL, use the permit or deny command to add new rules to the bottom of the list.
To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.

An ACL can contain up to 128 rules.

**Example**

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

**Related Commands**

- `permit`, `deny`, `redirect-to` (365)
- `mac access-group` (369)
- `show mac access-list` (370)

**permit, deny (MAC ACL)**

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

**Syntax**

```
{permit | deny}
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
[cos cos cos-bitmask] [vid vid vid-bitmask]
[ethertype protocol [protocol-bitmask]]
{(ip {any | host source-ip | source-ip network-mask}
 {any | host destination-ip | destination-ip network-mask})
{ipv6 {any | host source-ipv6 | source-ipv6/prefix-length}
 {any | host destination-ipv6 | destination-ipv6/prefix-length})
[protocol protocol]
[l4-source-port sport [port-bitmask]]
[l4-destination-port dport [port-bitmask]]
[time-range time-range-name]
```

**no**

```
{permit | deny | redirect-to interface}
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
[cos cos cos-bitmask] [vid vid vid-bitmask]
[ethertype protocol [protocol-bitmask]]
{(ip {any | host source-ip | source-ip network-mask}
 {any | host destination-ip | destination-ip network-mask})
{ipv6 {any | host source-ipv6 | source-ipv6/prefix-length}
 {any | host destination-ipv6 | destination-ipv6/prefix-length})
[protocol protocol]
[l4-source-port sport [port-bitmask]]
[l4-destination-port dport [port-bitmask]]
```
Note: The default is for Ethernet II packets.

{permit | deny} tagged-eth2
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
{cos cos cos-bitmask} [vid vid vid-bitmask]
[ethertype protocol [protocol-bitmask]]
{[ip {any | host source-ip | source-ip network-mask]}
  {any | host destination-ip | destination-ip network-mask]}
{ipv6 {any | host source-ipv6 | source-ipv6/prefix-length]}
  {any | host destination-ipv6 | destination-ipv6/prefix-length]}
[protocol protocol]
[l4-source-port sport [port-bitmask]]
[l4-destination-port dport [port-bitmask]]
[time-range time-range-name]

no {permit | deny} tagged-eth2
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask]
{cos cos cos-bitmask} [vid vid vid-bitmask]
[ethertype protocol [protocol-bitmask]]
{[ip {any | host source-ip | source-ip network-mask]}
  {any | host destination-ip | destination-ip network-mask]}
{ipv6 {any | host source-ipv6 | source-ipv6/prefix-length]}
  {any | host destination-ipv6 | destination-ipv6/prefix-length]}
[protocol protocol]
[l4-source-port sport [port-bitmask]]
[l4-destination-port dport [port-bitmask]]

{permit | deny} untagged-eth2
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask]
[ethertype protocol [protocol-bitmask]]
{[ip {any | host source-ip | source-ip network-mask]}
  {any | host destination-ip | destination-ip network-mask]}
{ipv6 {any | host source-ipv6 | source-ipv6/prefix-length]}
  {any | host destination-ipv6 | destination-ipv6/prefix-length]}
[protocol protocol]
[l4-source-port sport [port-bitmask]]
[l4-destination-port dport [port-bitmask]]
[time-range time-range-name]

no {permit | deny} untagged-eth2
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask]
[ethertype protocol [protocol-bitmask]]
{[ip {any | host source-ip | source-ip network-mask]}
  {any | host destination-ip | destination-ip network-mask]}

{ipv6 {any | host source-ipv6 | source-ipv6/prefix-length} 
  {any | host destination-ipv6 | destination-ipv6/prefix-length}}
[protocol protocol]
[l4-source-port sport [port-bitmask]]
[l4-destination-port dport [port-bitmask]]

(permit | deny) tagged-802.3
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
[cos cos cos-bitmask] [vid vid vid vid-bitmask]
[time-range time-range-name]

no (permit | deny) tagged-802.3
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
[cos cos cos-bitmask] [vid vid vid vid-bitmask]

(permit | deny) untagged-802.3
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
[time-range time-range-name]

no (permit | deny) untagged-802.3
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}

tagged-eth2 – Tagged Ethernet II packets.
untagged-eth2 – Untagged Ethernet II packets.
tagged-802.3 – Tagged Ethernet 802.3 packets.
untagged-802.3 – Untagged Ethernet 802.3 packets.
any – Any MAC source or destination address.
host – A specific MAC address.
source – Source MAC, IPv4 or IPv6 address.
destination – Destination MAC, IPv4 or IPv6 address.
address-bitmask\(^5\) – Bitmask for MAC address (in hexadecimal format).
network-mask – Network mask for IP subnet. This mask identifies the host
address bits used for routing to specific subnets.

prefix-length - Length of IPv6 prefix. A decimal value indicating how many
contiguous bits (from the left) of the address comprise the prefix; i.e., the
network portion of the address. (Range: 0-128)
cos – Class-of-Service value (Range: 0-7)
cos-bitmask\(^5\) – Class-of-Service bitmask. (Range: 0-7)
vid – VLAN ID. (Range: 1-4094)
vid-bitmask\(^5\) – VLAN bitmask. (Range: 1-4095)
ethtype – A specific Ethernet protocol number. (Range: 0-ffff hex)

\(^5\) For all bitmasks, “1” means care and “0” means ignore.
ethertype-bitmask$^5$ – Protocol bitmask. (Range: 0-ffff hex)

protocol - IP protocol. (Range: 0-255)

protocol-bitmask$^5$ – Protocol bitmask. (Range: 600-ffff hex.)

sport$^6$ – Protocol source port number. (Range: 0-65535)

dport$^6$ – Protocol destination port number. (Range: 0-65535)

port-bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

time-range-name - Name of the time range. (Range: 1-32 characters)

**Default Setting**
None

**Command Mode**
MAC ACL

**Command Usage**

◆ New rules are added to the end of the list.

◆ The **ethertype** option can only be used to filter Ethernet II formatted packets.

◆ A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:

- 0800 - IP
- 0806 - ARP
- 8137 - IPX

**Example**

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

**Related Commands**
access-list mac (364)
Time Range (155)

---

$^5$ Includes TCP, UDP or other protocol types.
**mac access-group**  This command binds a MAC ACL to a port. Use the **no** form to remove the port.

**Syntax**

```
mac access-group acl-name in [time-range time-range-name] [counter]
```

- `acl-name` – Name of the ACL. (Maximum length: 32 characters)
- `in` – Indicates that this list applies to ingress packets.
- `time-range-name` - Name of the time range. (Range: 1-16 characters)
- `counter` – Enables counter for ACL statistics.

**Default Setting**

None

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

- Only one ACL can be bound to a port.
- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

**Example**

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

**Related Commands**

- `show mac access-list (370)`
- `Time Range (155)`

**show mac access-group**  This command shows the ports assigned to MAC ACLs.

**Command Mode**

Privileged Exec

**Example**

```
Console#show mac access-group
Interface ethernet 1/5
MAC access-list M5 in
Console#
```

**Related Commands**

- `mac access-group (369)`
**show mac access-list**  This command displays the rules for configured MAC ACLs.

**Syntax**

`show mac access-list [acl-name]`

`acl-name` – Name of the ACL. (Maximum length: 32 characters)

**Command Mode**

Privileged Exec

**Example**

```
Console#show mac access-list
MAC access-list jerry:
   permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

**Related Commands**

`permit, deny, redirect-to (365)`

`mac access-group (369)`

---

### ARP ACLs

The commands in this section configure ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the `ip arp inspection vlan` command (page 336).

**Table 68: ARP ACL Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list arp</td>
<td>Creates a ARP ACL and enters configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>permit, deny</td>
<td>Filters packets matching a specified source or destination address in ARP messages</td>
<td>ARP-ACL</td>
</tr>
<tr>
<td>show access-list arp</td>
<td>Displays the rules for configured ARP ACLs</td>
<td>PE</td>
</tr>
<tr>
<td>show arp access-list</td>
<td>Displays the rules for configured ARP ACLs</td>
<td>PE</td>
</tr>
</tbody>
</table>

**access-list arp**  This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

**Syntax**

`[no] access-list arp acl-name`

`acl-name` – Name of the ACL. (Maximum length: 32 characters)
Default Setting
None

Command Mode
Global Configuration

Command Usage
◆ When you create a new ACL or enter configuration mode for an existing ACL, use the `permit` or `deny` command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
◆ To remove a rule, use the `no permit` or `no deny` command followed by the exact text of a previously configured rule.
◆ An ACL can contain up to 128 rules.

Example
```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

Related Commands
`permit`, `deny` (371)
`show arp access-list` (373)

`permit`, `deny` (ARP ACL)
This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the `no` form to remove a rule.

Syntax
```
[no] {permit | deny} 
  ip {any | host source-ip | source-ip ip-address-bitmask} 
  mac {any | host source-mac | source-mac mac-address-bitmask} [log]
```
This form indicates either request or response packets.

```
[no] {permit | deny} request 
  ip {any | host source-ip | source-ip ip-address-bitmask} 
  mac {any | host source-mac | source-mac mac-address-bitmask} [log]
```

```
[no] {permit | deny} response 
  ip {any | host source-ip | source-ip ip-address-bitmask} 
  {any | host destination-ip | destination-ip ip-address-bitmask} 
  mac {any | host source-mac | source-mac mac-address-bitmask} 
  [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

`source-ip` – Source IP address.

`destination-ip` – Destination IP address with bitmask.
**Chapter 9 | Access Control Lists**

**ARP ACLs**

- **ip-address-bitmask** – IPv4 number representing the address bits to match.
- **source-mac** – Source MAC address.
- **destination-mac** – Destination MAC address range with bitmask.
- **mac-address-bitmask** – Bitmask for MAC address (in hexadecimal format).
- **log** - Logs a packet when it matches the access control entry.

**Default Setting**
None

**Command Mode**
ARP ACL

**Command Usage**
New rules are added to the end of the list.

**Example**
This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

```
Console(config-arp-acl)#permit response ip any 192.168.0.0 255.255.0.0 mac any any
```

**Related Commands**
- access-list arp (370)

**show access-list arp**
This command displays the rules for configured ARP ACLs.

**Syntax**

```
show access-list arp [acl-name]
```

- **acl-name** – Name of the ACL. (Maximum length: 32 characters)

**Command Mode**
Privileged Exec

**Example**

```
Console# show access-list arp
ARP access-list factory:
    permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

1. For all bitmasks, binary “1” means care and “0” means ignore.
show arp access-list  This command displays the rules for configured ARP ACLs.

Syntax

show arp access-list [acl-name]

acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode
Privileged Exec

Example

Console#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#

ACL Information

This section describes commands used to display ACL information.

Table 69: ACL Information Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear access-list hardware counters</td>
<td>Clears hit counter for rules in all ACLs, or in a specified ACL.</td>
<td>PE</td>
</tr>
<tr>
<td>show access-group</td>
<td>Shows the ACLs assigned to each port</td>
<td>PE</td>
</tr>
<tr>
<td>show access-list</td>
<td>Show all ACLs and associated rules</td>
<td>PE</td>
</tr>
</tbody>
</table>

clear access-list hardware counters  This command clears the hit counter for the rules in all ACLs, or for the rules in a specified ACL.

Syntax

clear access-list hardware counters

[direction [in | out] [interface interface]] | [interface interface] | [name acl-name]

in – Clears counter for ingress rules.
interface

`ethernet unit/port`

- `unit` - Unit identifier. (Range: 1)
- `port` - Port number. (Range: 1-28/52)

`acl-name` – Name of the ACL. (Maximum length: 32 characters)

**Command Mode**
Privileged Exec

**Example**

```console
Console# clear access-list hardware counters
Console#
```

**show access-group**  This command shows the port assignments of ACLs.

**Command Mode**
Privileged Executive

**Example**

```console
Console# show access-group
Interface ethernet 1/2
  IP access-list david
  MAC access-list jerry
Console#
```

**show access-list**  This command shows all ACLs and associated rules.

**Syntax**

```plaintext
show access-list
    [[arp [acl-name]] | [ip [extended [acl-name] | standard [acl-name]]] | [ipv6 [extended [acl-name] | standard [acl-name]]] | [mac [acl-name]] | [tcam-utilization] | [hardware counters]]
```

- `arp` – Shows ingress or egress rules for ARP ACLs.
- `hardware counters` – Shows statistics for all ACLs.\(^8\)
- `ip extended` – Shows ingress rules for Extended IPv4 ACLs.
- `ipv6 extended` – Shows ingress rules for Extended IPv6 ACLs.

\(^8\) Due to a hardware limitation, this option only displays statistics for permit rules.
**mac** – Shows ingress rules for MAC ACLs.

**tcam-utilization** – Shows the percentage of user configured ACL rules as a percentage of total ACL rules

**acl-name** – Name of the ACL. (Maximum length: 32 characters)

**Command Mode**
Privileged Exec

**Example**

```
Console#show access-list
IP standard access-list david:
    permit host 10.1.1.21
    permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
    permit 10.7.1.1 255.255.255.0 any
    permit 192.168.1.0 255.255.255.0 any destination-port 80 80
    permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
    permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
    deny tcp any any control-flag 2 2
    permit any any
Console#
```
Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

Table 70: Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface Configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>Configures an interface type and enters interface configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>alias</td>
<td>Configures an alias name for the interface</td>
<td>IC</td>
</tr>
<tr>
<td>capabilities</td>
<td>Advertises the capabilities of a given interface for use in autonegotiation</td>
<td>IC</td>
</tr>
<tr>
<td>description</td>
<td>Adds a description to an interface configuration</td>
<td>IC</td>
</tr>
<tr>
<td>flowcontrol</td>
<td>Enables flow control on a given interface</td>
<td>IC</td>
</tr>
<tr>
<td>media-type</td>
<td>Forces transceiver mode to use for ports</td>
<td>IC</td>
</tr>
<tr>
<td>negotiation</td>
<td>Enables autonegotiation of a given interface</td>
<td>IC</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables an interface</td>
<td>IC</td>
</tr>
<tr>
<td>speed-duplex</td>
<td>Configures the speed and duplex operation of a given interface when autonegotiation is disabled</td>
<td>IC</td>
</tr>
<tr>
<td>clear counters</td>
<td>Clears statistics on an interface</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces brief</td>
<td>Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces counters</td>
<td>Displays statistics for the specified interfaces</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays status for the specified interface</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays the administrative and operational status of an interface</td>
<td>NE, PE</td>
</tr>
<tr>
<td><strong>Transceiver Threshold Configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>transceiver-monitor</td>
<td>Sends a trap when any of the transceiver's operational values fall outside specified thresholds</td>
<td>IC</td>
</tr>
<tr>
<td>transceiver-threshold-auto</td>
<td>Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent</td>
<td>IC</td>
</tr>
<tr>
<td>transceiver-threshold current</td>
<td>Sets thresholds for transceiver current which can be used to trigger an alarm or warning message</td>
<td>IC</td>
</tr>
<tr>
<td>transceiver-threshold rx-power</td>
<td>Sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message</td>
<td>IC</td>
</tr>
</tbody>
</table>
Table 70: Interface Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>transceiver-threshold</td>
<td>Sets thresholds for the transceiver temperature which can temperature</td>
<td>IC</td>
</tr>
<tr>
<td>temperature</td>
<td>be used to trigger an alarm or warning message</td>
<td></td>
</tr>
<tr>
<td>tx-power</td>
<td>Sets thresholds for the transceiver power level of the transmitters</td>
<td>IC</td>
</tr>
<tr>
<td>voltage</td>
<td>which can be used to trigger an alarm or warning message</td>
<td></td>
</tr>
<tr>
<td>show interfaces transceiver</td>
<td>Displays the temperature, voltage, bias current, transmit power, and</td>
<td>PE</td>
</tr>
<tr>
<td></td>
<td>receive power</td>
<td></td>
</tr>
<tr>
<td>show interfaces transceiver-</td>
<td>Displays the alarm/warning thresholds for temperature, voltage, bias</td>
<td>PE</td>
</tr>
<tr>
<td>threshold</td>
<td>current, transmit power, and receive power</td>
<td></td>
</tr>
</tbody>
</table>

Cable Diagnostics

test cable-diagnostics      | Performs cable diagnostics on the specified port                        | PE   |
| show cable-diagnostics     | Shows the results of a cable diagnostics test                            | PE   |

Power Savings

power-save                  | Enables power savings mode on the specified port                        | IC   |
| show power-save            | Shows the configuration settings for power savings                       | PE   |

Power Savings

power-save                  | Enables power savings mode on the specified port                        | IC   |
| show power-save            | Shows the configuration settings for power savings                       | PE   |

Interface Configuration

interface                    | This command configures an interface type and enters interface configuration|      |
|                            | mode. Use the no form with a trunk to remove an inactive interface.       |      |

Syntax

[no] interface interface-list

interface-list – One or more ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)

vlan vlan-id (Range: 1-4094)

Default Setting
None

transceiver-threshold

Sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message.

transceiver-threshold voltage

Sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message.

show interfaces transceiver

Displays the temperature, voltage, bias current, transmit power, and receive power.

show interfaces transceiver-threshold

Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power.

test cable-diagnostics

Performs cable diagnostics on the specified port.

show cable-diagnostics

Shows the results of a cable diagnostics test.

power-save

Enables power savings mode on the specified port.

show power-save

Shows the configuration settings for power savings.
Command Mode
Global Configuration

Example
To specify several different ports, enter the following command:

```
Console(config)#interface ethernet 1/17-20,23
Console(config-if)#shutdown
```

**alias**
This command configures an alias name for the interface. Use the **no** form to remove the alias name.

**Syntax**

```
alias string
no alias
```

- **string** - A mnemonic name to help you remember what is attached to this interface. (Range: 1-64 characters)

**Default Setting**
None

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The alias is displayed in the running-configuration file. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface.

**Example**
The following example adds an alias to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#alias finance
Console(config-if)#
```

capabilities
This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

**Syntax**

```
[no] capabilities {10000full | 10000full | 1000full | 100full | 100half | 10full |
10half | flowcontrol}
```
**10000full** - Supports 10 Gbps full-duplex operation  
**1000full** - Supports 10 Gbps full-duplex operation  
**1000full** - Supports 10 Gbps full-duplex operation  
**100full** - Supports 1 Gbps full-duplex operation  
**100half** - Supports 1 Gbps half-duplex operation  
**10full** - Supports 10 Mbps full-duplex operation  
**10half** - Supports 10 Mbps half-duplex operation  
**flowcontrol** - Supports flow control  

**Default Setting**  
100BASE-FX: 100full (SFP)  
1000BASE-T: 10half, 10full, 100half, 100full, 1000full  
1000BASE-SX/LX/LH (SFP): 1000full  
10GBASE-SR/LR/ER (XFP): 10000full  

**Command Mode**  
Interface Configuration (Ethernet, Port Channel)  

**Command Usage**  
◆ The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.  
◆ When auto-negotiation is enabled with the `negotiation` command, the switch will negotiate the best settings for a link based on the `capabilities` command. When auto-negotiation is disabled, you must manually specify the link attributes with the `speed-duplex` and `flowcontrol` commands.  

**Example**  
The following example configures Ethernet port 5 capabilities to include 100half and 100full.  

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

**Related Commands**  
`negotiation (383)`  
`speed-duplex (384)`  
`flowcontrol (381)`
**description**  This command adds a description to an interface. Use the no form to remove the description.

**Syntax**

```
description string

no description
```

`string` - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

**Default Setting**
None

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The description is displayed by the `show interfaces status` command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

**Example**
The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
```
back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.

- To force flow control on or off (with the `flowcontrol` or `no flowcontrol` command), use the `no negotiation` command to disable auto-negotiation on the selected interface.

- When using the `negotiation` command to enable auto-negotiation, the optimal settings will be determined by the `capabilities` command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port.

**Example**
The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

**Related Commands**
negotiation (383)
capabilities (flowcontrol, symmetric) (379)

**media-type**  
This command forces the transceiver mode to use for ports. Use the `no` form to restore the default mode.

**Syntax**

```
media-type sfp-forced [mode]

no media-type
```

**Default Setting**
None

**Command Mode**
Interface Configuration (SFP Ports)

**Example**
This forces the switch to use the 1000sfp mode for SFP port 28.

```
Console(config)#interface ethernet 1/28
Console(config-if)#media-type sfp-forced 1000sfp
Console(config-if)#
```
**negotiation**  This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

**Syntax**

```
[no] negotiation
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

◆ 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.

◆ When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

◆ If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

**Example**

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

**Related Commands**

- **capabilities** (379)
- **speed-duplex** (384)

---

**shutdown**  This command disables an interface. To restart a disabled interface, use the **no** form.

**Syntax**

```
[no] shutdown
```

**Default Setting**

All interfaces are enabled.

**Command Mode**

Interface Configuration (Ethernet, Port Channel)
**Command Usage**
This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

**Example**
The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

**speed-duplex**  This command configures the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

**Syntax**
```
speed-duplex {10000full | 100full | 100half | 10full | 10half}
no speed-duplex 10000full - Forces 10 Gbps full-duplex operation
    10000full - Forces 10 Gbps full-duplex operation
    100full - Forces 100 Mbps full-duplex operation
    100half - Forces 100 Mbps half-duplex operation
    10full - Forces 10 Mbps full-duplex operation
    10half - Forces 10 Mbps half-duplex operation
```

**Default Setting**
◆  Auto-negotiation is enabled by default.
◆  When auto-negotiation is disabled, the default speed-duplex setting is **100full** for 1000BASE-T ports.
    ▪  10 Gigabit Ethernet ports – **10000full** (10 Gbps full-duplex)
    ▪  10 Gigabit Ethernet ports – **10000full** (10 Gbps full-duplex)

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
◆  The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
◆  To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
When using the `negotiation` command to enable auto-negotiation, the optimal settings will be determined by the `capabilities` command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

**Example**
The following example configures port 5 to 100 Mbps, half-duplex operation.

```plaintext
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

**Related Commands**
`negotiation (383)`
`capabilities (379)`

**clear counters**
This command clears statistics on an interface.

**Syntax**
```
clear counters interface
clear counters ethernet unit/port
```
- `interface`
- `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)
- `port-channel channel-id` (Range: 1-16)

**Default Setting**
None

**Command Mode**
Privileged Exec

**Command Usage**
Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

**Example**
The following example clears statistics on port 5.

```plaintext
Console#clear counters ethernet 1/5
Console#
```
**show interfaces brief**  This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

**Command Mode**  Privileged Exec

**Command Usage**
- If an SFP transceiver is inserted in a port, the Type field will show the SFP type as interpreted from Ethernet Compliance Codes (Data Byte 6 in Address A0h). The Ethernet Compliance Code is a bitmap value, of which one bit is supposedly turned on. However, if the read-out is not recognizable (e.g., 2 or more bits on, or all 0s), the Type field just displays the raw data (hexadecimal value).
- The Type field will always display “NA” for a trunk entry because a trunk allows for mixed port types such as 1000Base T and 1000Base SFP.

**Example**

```
Console#show interfaces brief
Interface Name               Status   PVID Pri Speed/Duplex  Type         Trunk
--------- ------------------ ------- ---- --- ------------- ----------- ----- 
Eth 1/ 1                     Up          1   0 Auto-100full  1000BASE-T    None
Eth 1/ 2                     Down        1   0 Auto          1000BASE-T    None
Eth 1/ 3                     Down        1   0 Auto          1000BASE-T    None
Eth 1/ 4                     Down        1   0 Auto          1000BASE-T    None
Eth 1/ 5                     Down        1   0 Auto          1000BASE-T    None
Eth 1/ 6                     Down        1   0 Auto          1000BASE-T    None
...
```

**show interfaces counters**  This command displays interface statistics.

**Syntax**

```
show interfaces counters [interface]
```

- **interface**
  - **ethernet unit/port**
    - **unit** - Unit identifier. (Range: 1)
    - **port** - Port number. (Range: 1-28/52)
  - **port-channel channel-id** (Range: 1-16)

**Default Setting**  Shows the counters for all interfaces.

**Command Mode**  Normal Exec, Privileged Exec
**Command Usage**

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Showing Port or Trunk Statistics” in the System Reference Guide.

**Example**

```
Console#show interfaces counters ethernet 1/17
Ethernet 1/ 17
====== IF table Stats ======
  2166458 Octets Input
  14734059 Octets Output
  14707 Unicast Input
  19806 Unicast Output
  0 Discard Input
  0 Discard Output
  0 Error Input
  0 Error Output
  0 Unknown Protocols Input
  0 QLen Output
====== Extended Iftable Stats ======
  23 Multi-cast Input
  5525 Multi-cast Output
  170 Broadcast Input
  11 Broadcast Output
====== Ether-like Stats ======
  0 Alignment Errors
  0 FCS Errors
  0 Single Collision Frames
  0 Multiple Collision Frames
  0 SQE Test Errors
  0 Deferred Transmissions
  0 Late Collisions
  0 Excessive Collisions
  0 Internal Mac Transmit Errors
  0 Internal Mac Receive Errors
  0 Frames Too Long
  0 Carrier Sense Errors
  0 Symbol Errors
  0 Pause Frames Input
  0 Pause Frames Output
====== RMON Stats ======
  0 Drop Events
  16900558 Octets
  40243 Packets
  170 Broadcast PKTS
  23 Multi-cast PKTS
  0 Undersize PKTS
  0 Oversize PKTS
  0 Fragments
  0 Jabbers
  0 CRC Align Errors
  0 Collisions
  21065 Packet Size <= 64 Octets
  3805 Packet Size 65 to 127 Octets
  2448 Packet Size 128 to 255 Octets
  797 Packet Size 256 to 511 Octets
  2941 Packet Size 512 to 1023 Octets
  9187 Packet Size 1024 to 1518 Octets
====== Port Utilization (recent 300 seconds) ======
  0 Octets Input in kbits per second
  0 Packets Input per second
  0.00 % Input Utilization
```
show interfaces status  This command displays the status for an interface.

Syntax

show interfaces status [interface]

interface

  ethernet unit/port

    unit - Unit identifier. (Range: 1)

    port - Port number. (Range: 1-28/52)

  port-channel channel-id (Range: 1-16)

  vlan vlan-id (Range: 1-4094)

Default Setting
Shows the status for all interfaces.

Command Mode
Normal Exec, Privileged Exec

Command Usage
If no interface is specified, information on all interfaces is displayed.

Example

Console# show interfaces status ethernet 1/21
Information of Eth 1/21
  Port Type : 1000BASE-T
  MAC Address : B4-0E-DC-34-E6-3D
Configuration:
  Name : 
  Port Admin : Up
  Speed-Duplex : Auto
  Capabilities : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm : Enabled
  Broadcast Storm Limit : 500 packets/second
  Multicast Storm : Disabled
  Multicast Storm Limit : 500 packets/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Flow Control : Disabled
  VLAN Trunking : Disabled
  LACP : Disabled
  Media Type : None
  Giga PHY Mode : Master
  Current Status:
  Link Status : Up
show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [interface]

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 21.

Console#show interfaces switchport ethernet 1/21
Information of Eth 1/21
Broadcast Threshold : Enabled, 500 packets/second
Multicast Threshold : Disabled
Unknown Unicast Threshold : Disabled
LACP Status : Disabled
Ingress Rate Limit : Disabled, 1000M bits per second
Egress Rate Limit : Disabled, 1000M bits per second
VLAN Membership Mode : Hybrid
Ingress Rule : Disabled
Acceptable Frame Type : All frames
Native VLAN : 1
Priority for Untagged Traffic : 0
GVRP Status : Disabled
Allowed VLAN : 1(u)
Forbidden VLAN :
802.1Q-Tunnel Status : Disable
802.1Q-Tunnel Mode : NORMAL
802.1Q-Tunnel TPID : 8100(Hex)
Layer 2 Protocol Tunnel : None
Console#
**Table 71: show interfaces switchport - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast Threshold</td>
<td>Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 437).</td>
</tr>
<tr>
<td>Multicast Threshold</td>
<td>Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 437).</td>
</tr>
<tr>
<td>Unknown Unicast Threshold</td>
<td>Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 437).</td>
</tr>
<tr>
<td>LACP Status</td>
<td>Shows if Link Aggregation Control Protocol has been enabled or disabled (page 406).</td>
</tr>
<tr>
<td>Ingress/Egress Rate Limit</td>
<td>Shows if rate limiting is enabled, and the current rate limit (page 765).</td>
</tr>
<tr>
<td>VLAN Membership Mode</td>
<td>Indicates membership mode as Trunk or Hybrid (page 508).</td>
</tr>
<tr>
<td>Ingress Rule</td>
<td>Shows if ingress filtering is enabled or disabled (page 507).</td>
</tr>
<tr>
<td>Acceptable Frame Type</td>
<td>Shows if acceptable VLAN frames include all types or tagged frames only (page 505).</td>
</tr>
<tr>
<td>Native VLAN</td>
<td>Indicates the default Port VLAN ID (page 509).</td>
</tr>
<tr>
<td>Priority for Un tagged Traffic</td>
<td>Indicates the default priority for untagged frames (page 544).</td>
</tr>
<tr>
<td>GVRP Status</td>
<td>Shows if GARP VLAN Registration Protocol is enabled or disabled (page 499).</td>
</tr>
<tr>
<td>Allowed VLAN</td>
<td>Shows the VLANs this interface has joined, where &quot;(u)&quot; indicates untagged and &quot;(t)&quot; indicates tagged (page 506).</td>
</tr>
<tr>
<td>Forbidden VLAN</td>
<td>Shows the VLANs this interface can not dynamically join via GVRP (page 498).</td>
</tr>
<tr>
<td>802.1Q-tunnel Status</td>
<td>Shows if 802.1Q tunnel is enabled on this interface (page 515).</td>
</tr>
<tr>
<td>802.1Q-tunnel Mode</td>
<td>Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 517).</td>
</tr>
<tr>
<td>802.1Q-tunnel TPID</td>
<td>Shows the Tag Protocol Identifier used for learning and switching packets (page 516).</td>
</tr>
<tr>
<td>Layer 2 Protocol Tunnel</td>
<td>Shows if L2 Protocol Tunnel is enabled for spanning tree protocol (page 524).</td>
</tr>
</tbody>
</table>

**Transceiver Threshold Configuration**

**transceiver-monitor**

This command sends a trap when any of the transceiver’s operational values fall outside of specified thresholds. Use the **no** form to disable trap messages.

**Syntax**

```
transceiver-monitor
```

**Default Setting**

Enabled
Chapter 10 | Interface Commands
Transceiver Threshold Configuration

**Command Mode**
Interface Configuration (Ports)

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-monitor
Console#
```

**transceiver-threshold-auto**
This command uses default threshold settings obtained from the transceiver to determine when an alarm or warning message should be sent. Use the no form to disable this feature.

**Syntax**

```
transceiver-threshold-auto
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ports)

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold-auto
Console#
```

**transceiver-threshold-current**
This command sets thresholds for transceiver current which can be used to trigger an alarm or warning message.

**Syntax**

```
transceiver-threshold-current \{high-alarm | high-warning \} \{low-alarm | low-warning\} threshold-value
```

- **high-alarm** – Sets the high current threshold for an alarm message.
- **high-warning** – Sets the high current threshold for a warning message.
- **low-alarm** – Sets the low current threshold for an alarm message.
- **low-warning** – Sets the low current threshold for a warning message.

**threshold-value** – The threshold of the transceiver current.
(Range: 0-13100 in units of 0.01 mA)

**Default Setting**

- High Alarm: 100 mA
- High Warning: 90 mA
Low Warning: 7 mA  
Low Alarm: 6 mA

**Command Mode**

Interface Configuration (Ports)

**Command Usage**

◆ If trap messages are enabled with the `transceiver-monitor` command, and a high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.

◆ If trap messages are enabled with the `transceiver-monitor` command, and a low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.

◆ Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.

◆ Trap messages enabled by the `transceiver-monitor` command are sent to any management station configured by the `snmp-server host` command.

**Example**
The following example sets alarm thresholds for the transceiver current at port 1.

```bash
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold current low-alarm 100
Console(config-if)#transceiver-threshold rx-power high-alarm 700
Console#
```
transceiver-threshold rx-power

This command sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message.

Syntax

```
transceiver-threshold rx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value
```

- `high-alarm` – Sets the high power threshold for an alarm message.
- `high-warning` – Sets the high power threshold for a warning message.
- `low-alarm` – Sets the low power threshold for an alarm message.
- `low-warning` – Sets the low power threshold for a warning message.

`threshold-value` – The power threshold of the received signal.
(Range: -4000 - 820 in units of 0.01 dBm)

Default Setting

- High Alarm: -3.00 dBm
- High Warning: -3.50 dBm
- Low Warning: -21.00 dBm
- Low Alarm: -21.50 dBm

Command Mode

Interface Configuration (Ports)

Command Usage

- The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

- Refer to the Command Usage section under the `transceiver-threshold current` command for more information on configuring transceiver thresholds.

- Trap messages enabled by the `transceiver-monitor` command are sent to any management station configured by the `snmp-server host` command.

Example

The following example sets alarm thresholds for the signal power received at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold rx-power low-alarm -21
Console(config-if)#transceiver-threshold rx-power high-alarm -3
Console#`
```
transceiver-threshold temperature

This command sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message.

Syntax

```
transceiver-threshold temperature {high-alarm | high-warning | low-alarm | low-warning} threshold-value
```

- **high-alarm** – Sets the high temperature threshold for an alarm message.
- **high-warning** – Sets the high temperature threshold for a warning message.
- **low-alarm** – Sets the low temperature threshold for an alarm message.
- **low-warning** – Sets the low temperature threshold for a warning message.

**threshold-value** – The threshold of the transceiver temperature.
(Range: -12800 - 12800 in units of 0.01 Celsius)

Default Setting

- High Alarm: 75.00 °C
- High Warning: 70.00 °C
- Low Alarm: -123.00 °C
- Low Warning: 0.00 °C

Command Mode

Interface Configuration (Ports)

Command Usage

- Refer to the Command Usage section under the transceiver-threshold current command for more information on configuring transceiver thresholds.

- Trap messages enabled by the transceiver-monitor command are sent to any management station configured by the snmp-server host command.

Example

The following example sets alarm thresholds for the transceiver temperature at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold temperature low-alarm 97
Console(config-if)#transceiver-threshold temperature high-alarm -83
Console#```
This command sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message.

**Syntax**

```plaintext
transceiver-threshold tx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value
```

- `high-alarm` – Sets the high power threshold for an alarm message.
- `high-warning` – Sets the high power threshold for a warning message.
- `low-alarm` – Sets the low power threshold for an alarm message.
- `low-warning` – Sets the low power threshold for a warning message.

`threshold-value` – The power threshold of the transmitted signal.

(Range: -4000 - 820 in units of 0.01 dBm)

**Default Setting**

- High Alarm: -9.00 dBm
- High Warning: -9.50 dBm
- Low Warning: -21.00 dBm
- Low Alarm: -21.50 dBm

**Command Mode**

Interface Configuration (Ports)

**Command Usage**

- The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

- Refer to the Command Usage section under the `transceiver-threshold current` command for more information on configuring transceiver thresholds.

- Trap messages enabled by the `transceiver-monitor` command are sent to any management station configured by the `snmp-server host` command.

**Example**

The following example sets alarm thresholds for the signal power transmitted at port 1.

```plaintext
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold tx-power low-alarm 8
Console(config-if)#transceiver-threshold tx-power high-alarm -3
Console#"
```
transceiver-threshold voltage

This command sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message.

Syntax

```
transceiver-threshold voltage {high-alarm | high-warning | low-alarm | low-warning} threshold-value
```

- high-alarm – Sets the high voltage threshold for an alarm message.
- high-warning – Sets the high voltage threshold for a warning message.
- low-alarm – Sets the low voltage threshold for an alarm message.
- low-warning – Sets the low voltage threshold for a warning message.

threshold-value – The threshold of the transceiver voltage.
(Range: 0-655 in units of 0.01 Volt)

Default Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Alarm</td>
<td>3.50 Volts</td>
</tr>
<tr>
<td>High Warning</td>
<td>3.45 Volts</td>
</tr>
<tr>
<td>Low Warning</td>
<td>3.15 Volts</td>
</tr>
<tr>
<td>Low Alarm</td>
<td>3.10 Volts</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration (Ports)

Command Usage

- Refer to the Command Usage section under the `transceiver-threshold current` command for more information on configuring transceiver thresholds.
- Trap messages enabled by the `transceiver-monitor` command are sent to any management station configured by the `snmp-server host` command.

Example

The following example sets alarm thresholds for the transceiver voltage at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold voltage low-alarm 4
Console(config-if)#transceiver-threshold voltage high-alarm 2
Console#  
```
show interfaces transceiver

This command displays identifying information for the specified transceiver, including connector type and vendor-related parameters, as well as the temperature, voltage, bias current, transmit power, and receive power.

Syntax

```
show interfaces transceiver [interface]

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. ()
```

Default Setting

Shows all SFP interfaces.

Command Mode

Privileged Exec

Command Usage

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, and received optical power, and related alarm thresholds.

Example

```
Console#show interfaces transceiver ethernet 1/25
Information of Eth 1/25
Connector Type        : LC
Fiber Type            : [0x00]
Eth Compliance Codes  : 1000BASE-ZX
Baud Rate             : 1300 Mb/s
Vendor OUI            : 00-00-5F
Vendor Name           : SumitomoElectric
Vendor PN             : SCP6G94-FN-EWH
Vendor Rev            : Z
Vendor SN             : SE08T71200006
Date Code             : 10-09-14
DDM Info
Temperature         : 35.64 degree C
Vcc                 : 3.25 V
Bias Current        : 12.13 mA
TX Power            : 2.36 dBm
RX Power            : -24.20 dBm
DDM Thresholds

<table>
<thead>
<tr>
<th></th>
<th>Low Alarm</th>
<th>Low Warning</th>
<th>High Warning</th>
<th>High Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature(Celsius)</td>
<td>-45.00</td>
<td>-40.00</td>
<td>85.00</td>
<td>90.00</td>
</tr>
<tr>
<td>Voltage(Volts)</td>
<td>2.90</td>
<td>3.00</td>
<td>3.60</td>
<td>3.70</td>
</tr>
<tr>
<td>Current(mA)</td>
<td>1.00</td>
<td>3.00</td>
<td>50.00</td>
<td>60.00</td>
</tr>
<tr>
<td>TxPower(dBm)</td>
<td>-11.50</td>
<td>-10.50</td>
<td>-2.00</td>
<td>-1.00</td>
</tr>
</tbody>
</table>
```
show interfaces transceiver-threshold

This command Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power. Syntax

**Syntax**

```
show interfaces transceiver-threshold [interface]
```

```
interface
```

```
ethernet unit/port
```

```
unit - Unit identifier. (Range: 1)
```

```
port - Port number. ()
```

**Default Setting**

Shows all SFP interfaces.

**Command Mode**

Privileged Exec

**Command Usage**

- The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, received optical power, and related alarm thresholds.

- The DDM thresholds displayed by this command only apply to ports which have a DDM-compliant transceiver inserted.

**Example**

```
Console#show interfaces transceiver-threshold ethernet 1/25
Information of Eth 1/25
DDM Thresholds
Transceiver-monitor : Disabled
Transceiver-threshold-auto : Enabled

---------------------------------  ------  ------  ------  ------
Temperature(Celsius)            -123.00  0.00  70.00  75.00
Voltage(Volts)                 3.10  3.15  3.45  3.50
Current(mA)                    6.00  7.00  90.00  100.00
TxPower(dBm)                   -12.00  -11.50  -9.50  -9.00
RxPower(dBm)                   -21.50  -21.00  -3.50  -3.00

Console#
```
**Cable Diagnostics**

**test cable-diagnostics**  This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

**Syntax**

```
test cable-diagnostics interface interface

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-24/48)
```

**Command Mode**

Privileged Exec

**Command Usage**

◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test methods when the port link-up speed is 1 Gbps. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse. If the port link-up speed is not 1 Gbps, then Time Domain Reflectometry (TDR) test method is used. TDR also detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. However, TDR can only determine if a link is valid or faulty.

◆ This cable test is only accurate for Gigabit Ethernet cables 7 - 100 meters long.

◆ The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length of each cable pair.

◆ Potential conditions which may be listed by the diagnostics include:
  ■ OK: Correctly terminated pair
  ■ Open: Open pair, no link partner
  ■ Short: Shorted pair
  ■ Not Supported: This message is displayed for Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
  ■ Impedance mismatch: Terminating impedance is not in the reference range.

◆ Ports are linked down while running cable diagnostics.

◆ To ensure more accurate measurement of the length to a fault, first disable power-saving mode (using the no power-save command) on the link partner before running cable diagnostics.
**Example**

```
Console#test cable-diagnostics interface ethernet 1/23
Console#show cable-diagnostics interface ethernet 1/23
Port     Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -----------------
Eth 1/23   GE  Up          OK (21)          OK (21)          2009-11-13 09:44:19
Console#
```

**show cable-diagnostics**  This command shows the results of a cable diagnostics test.

**Syntax**

```
show cable-diagnostics interface [interface]

interface

ethernet unit/port

  unit - Unit identifier. (Range: 1)
  port - Port number. (Range: 1-24/48)
```

**Command Mode**

Privileged Exec

**Command Usage**

- The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.

- To ensure more accurate measurement of the length to a fault, first disable power-saving mode on the link partner before running cable diagnostics.

- For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.

**Example**

```
Console#show cable-diagnostics interface ethernet 1/23
Port     Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -----------------
Eth 1/23   GE  Up          OK (21)          OK (21)          2009-11-13 09:44:19
Console#
```
Power Savings

power-save  This command enables power savings mode on the specified port.

Syntax

[no] power-save

Command Mode
Interface Configuration (Ethernet, Ports 1-24/48)

Command Usage

◆ IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.

◆ Power saving mode only applies to the Gigabit Ethernet ports using copper media.

◆ Power savings can be enabled on Gigabit Ethernet RJ-45 ports.

◆ The power-saving methods provided by this switch include:
  
  ▪ Power saving when there is no link partner:
Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

  ▪ Power saving when there is a link partner:
Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to determine whether or not it can reduce the signal amplitude used on a particular link.
Note: Power savings can only be implemented on Gigabit Ethernet ports using twisted-pair cabling. Power-savings mode on an active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

Example

```console
Console(config)#interface ethernet 1/1
Console(config-if)#power-save
Console(config-if)#
```

show power-save  This command shows the configuration settings for power savings.

Syntax

```plaintext
show power-save [interface interface]

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-24/48)
```

Command Mode

Privileged Exec

Example

```console
Console#show power-save interface ethernet 1/4
Power Saving Status:
  Ethernet 1/1   : Enabled
Console#
```
Port Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 12 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 72: Link Aggregation Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manual Configuration Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Configures a trunk and enters interface configuration mode for the trunk</td>
<td>GC</td>
</tr>
<tr>
<td>port-channel load-balance</td>
<td>Sets the load-distribution method among ports in aggregated links</td>
<td>GC</td>
</tr>
<tr>
<td>channel-group</td>
<td>Adds a port to a trunk</td>
<td>IC (Ethernet)</td>
</tr>
<tr>
<td><strong>Dynamic Configuration Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lACP</td>
<td>Configures LACP for the current interface</td>
<td>IC (Ethernet)</td>
</tr>
<tr>
<td>lACP admin-key</td>
<td>Configures a port's administration key</td>
<td>IC (Ethernet)</td>
</tr>
<tr>
<td>lACP port-priority</td>
<td>Configures a port's LACP port priority</td>
<td>IC (Ethernet)</td>
</tr>
<tr>
<td>lACP system-priority</td>
<td>Configures a port's LACP system priority</td>
<td>IC (Ethernet)</td>
</tr>
<tr>
<td>lACP admin-key</td>
<td>Configures an port channel's administration key</td>
<td>IC (Port Channel)</td>
</tr>
<tr>
<td>lACP timeout</td>
<td>Configures the timeout to wait for next LACPDU</td>
<td>IC (Port Channel)</td>
</tr>
<tr>
<td><strong>Trunk Status Display Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show interfaces status port-channel</td>
<td>Shows trunk information</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show lACP</td>
<td>Shows LACP information</td>
<td>PE</td>
</tr>
<tr>
<td>show port-channel load-balance</td>
<td>Shows the load-distribution method used on aggregated links</td>
<td>PE</td>
</tr>
</tbody>
</table>

Guidelines for Creating Trunks

**General Guidelines** –

- Finish configuring trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
The ports at both ends of a connection must be configured as trunk ports.

All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.

Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.

All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.

STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

**Dynamically Creating a Port Channel**

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

**Manual Configuration Commands**

**port-channel**

This command sets the load-distribution method among ports in aggregated links (for both static and dynamic trunks). Use the `no` form to restore the default setting.

**Syntax**

```
port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}
```

**no port channel load-balance**

- **dst-ip** - Load balancing based on destination IP address.
- **dst-mac** - Load balancing based on destination MAC address.
- **src-dst-ip** - Load balancing based on source and destination IP address.
- **src-dst-mac** - Load balancing based on source and destination MAC address.
- **src-ip** - Load balancing based on source IP address.
- **src-mac** - Load balancing based on source MAC address.
Default Setting
src-dst-ip

Command Mode
Global Configuration

Command Usage
◆ This command applies to all static and dynamic trunks on the switch.

◆ To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:

- **dst-ip**: All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.

- **dst-mac**: All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.

- **src-dst-ip**: All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.

- **src-dst-mac**: All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.

- **src-ip**: All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.

- **src-mac**: All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

Example

```
Console(config)#port-channel load-balance dst-ip
Console(config)#
```
**channel-group**  This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

**Syntax**

```plaintext
channel-group channel-id
no channel-group
```

- `channel-id` - Trunk index (Range: 1-16)

**Default Setting**
The current port will be added to this trunk.

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**

◆ When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.

◆ Use **no channel-group** to remove a port group from a trunk.

◆ Use **no interface port-channel** to remove a trunk from the switch.

**Example**
The following example creates trunk 1 and then adds port 11:

```plaintext
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

---

**Dynamic Configuration Commands**

**lacp**  This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

**Syntax**

```plaintext
[no] lacp
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet)
Command Usage

◆ The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

◆ A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.

◆ If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

◆ If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the `show interfaces status port-channel 1` command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
```

Information of Trunk 1

<table>
<thead>
<tr>
<th>Basic Information:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>1000T</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00-E0-0C-00-00-FF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Port Admin</td>
<td>Up</td>
</tr>
<tr>
<td>Speed-Duplex</td>
<td>Auto</td>
</tr>
<tr>
<td>Capabilities</td>
<td>10half, 10full, 100half, 100full, 1000full</td>
</tr>
<tr>
<td>Broadcast Storm</td>
<td>Enabled</td>
</tr>
<tr>
<td>Broadcast Storm Limit</td>
<td>500 packets/second</td>
</tr>
<tr>
<td>Multicast Storm</td>
<td>Disabled</td>
</tr>
<tr>
<td>Multicast Storm Limit</td>
<td>500 packets/second</td>
</tr>
<tr>
<td>Unknown Unicast Storm</td>
<td>Disabled</td>
</tr>
<tr>
<td>Unknown Unicast Storm Limit</td>
<td>500 packets/second</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLAN Trunking</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC Learning</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Current Status:

<table>
<thead>
<tr>
<th>Created By</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Status</td>
<td>Up</td>
</tr>
<tr>
<td>Port Operational Status</td>
<td>Up</td>
</tr>
<tr>
<td>Operational Speed-Duplex</td>
<td>100full</td>
</tr>
<tr>
<td>Member Ports</td>
<td>Eth1/10, Eth1/11, Eth1/12,</td>
</tr>
</tbody>
</table>

Console#
**lacp admin-key** (Ethernet Interface) This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

**Syntax**

```plaintext
lacp {actor | partner} admin-key key
no lacp {actor | partner} admin-key
```

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- **key** - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

**Default Setting**
Actor: 1, Partner: 0

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).

- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.

- By default, the actor's operational key is determined by port's link speed (1000f - 4, 100f - 3, 10f - 2), and copied to the admin key.

**Example**

```plaintext
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```
**lacp port-priority**  This command configures LACP port priority. Use the **no** form to restore the default setting.

**Syntax**

```
lacp {actor | partner} port-priority priority
no lacp {actor | partner} port-priority
```

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- **priority** - LACP port priority is used to select a backup link. (Range: 0-65535)

**Default Setting**

32768

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

- Setting a lower value indicates a higher effective priority.

- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.

- If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```
**lacp system-priority**  This command configures a port’s LACP system priority. Use the **no** form to restore the default setting.

**Syntax**

```
lacp {actor | partner} system-priority priority
no lacp {actor | partner} system-priority
```

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- **priority** - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

**Default Setting**

32768

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch’s MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

**lacp admin-key**  This command configures a port channel’s LACP administration key string. Use the **no** form to restore the default setting.

**Syntax**

```
lacp admin-key key
no lacp admin-key
```

- **key** - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)
Default Setting

0

Command Mode
Interface Configuration (Port Channel)

Command Usage
◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).

◆ If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

◆ If the port channel admin key is set to a non-default value, the operational key is based upon LACP PDUs received from the partner, and the channel admin key is reset to the default value. The trunk identifier will also be changed by this process.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

**lacp timeout** This command configures the timeout to wait for the next LACP data unit (LACPDU). Use the no form to restore the default setting.

Syntax

```
lacp timeout {long | short}
no lacp timeout
```

**Default Setting**

**long**

**Command Mode**
Interface Configuration (Port Channel)

**Command Usage**
◆ The timeout configured by this command is set in the LACP timeout bit of the Actor State field in transmitted LACPDU. When the partner switch receives an
LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds.

◆ If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group.

◆ When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port.

◆ When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp timeout short
Console(config-if)#
```

Trunk Status Display Commands

**show lacp**  This command displays LACP information.

**Syntax**

```
show lacp [port-channel] {counters | internal | neighbors | sys-id}
```

- **port-channel**: Local identifier for a link aggregation group. (Range: 1-12)
- **counters**: Statistics for LACP protocol messages.
- **internal**: Configuration settings and operational state for local side.
- **neighbors**: Configuration settings and operational state for remote side.
- **sys-id**: Summary of system priority and MAC address for all channel groups.

**Default Setting**

- Port Channel: all

**Command Mode**

- Privileged Exec
Example

```
Example

console#show lacp 1 counters
Port Channel: 1

Eth 1/2

LACPDUs Sent : 12
LACPDUs Received : 6
Marker Sent : 0
Marker Received : 0
LACPDUs Unknown Pkts : 0
LACPDUs Illegal Pkts : 0
```

```
Table 73: show lacp counters - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACPDUs Sent</td>
<td>Number of valid LACPDUs transmitted from this channel group.</td>
</tr>
<tr>
<td>LACPDUs Received</td>
<td>Number of valid LACPDUs received on this channel group.</td>
</tr>
<tr>
<td>Marker Sent</td>
<td>Number of valid Marker PDUs transmitted from this channel group.</td>
</tr>
<tr>
<td>Marker Received</td>
<td>Number of valid Marker PDUs received by this channel group.</td>
</tr>
<tr>
<td>LACPDUs Unknown Pkts</td>
<td>Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.</td>
</tr>
<tr>
<td>LACPDUs Illegal Pkts</td>
<td>Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.</td>
</tr>
</tbody>
</table>
```

```
Example

console#show lacp 1 internal
Port Channel : 1

Oper Key : 3
Admin Key : 0
Timeout : long

Eth 1/1

LACPDUs Internal : 30 seconds
LACP System Priority : 32768
LACP Port Priority : 32768
Admin Key : 3
Oper Key : 3
Admin State : defaulted, aggregation, long timeout, LACP-activity
Oper State : distributing, collecting, synchronization, aggregation, long timeout, LACP-activity
```

```
Table 74: show lacp internal - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper Key</td>
<td>Current operational value of the key for the aggregation port.</td>
</tr>
<tr>
<td>Admin Key</td>
<td>Current administrative value of the key for the aggregation port.</td>
</tr>
<tr>
<td>LACPDUs Internal</td>
<td>Number of seconds before invalidating received LACPDU information.</td>
</tr>
</tbody>
</table>
```
### Table 74: show lacp internal - display description (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP System Priority</td>
<td>LACP system priority assigned to this port channel.</td>
</tr>
<tr>
<td>LACP Port Priority</td>
<td>LACP port priority assigned to this interface within the channel group.</td>
</tr>
<tr>
<td>Admin State, Oper State</td>
<td>Administrative or operational values of the actor’s state parameters:</td>
</tr>
<tr>
<td></td>
<td>◦ Expired – The actor’s receive machine is in the expired state;</td>
</tr>
<tr>
<td></td>
<td>◦ Defaulted – The actor’s receive machine is using defaulted operational</td>
</tr>
<tr>
<td></td>
<td>partner information, administratively configured for the partner.</td>
</tr>
<tr>
<td></td>
<td>◦ Distributing – If false, distribution of outgoing frames on this link is</td>
</tr>
<tr>
<td></td>
<td>disabled; i.e., distribution is currently disabled and is not expected</td>
</tr>
<tr>
<td></td>
<td>to be enabled in the absence of administrative changes or changes in</td>
</tr>
<tr>
<td></td>
<td>received protocol information.</td>
</tr>
<tr>
<td></td>
<td>◦ Collecting – Collection of incoming frames on this link is enabled; i.e.,</td>
</tr>
<tr>
<td></td>
<td>collection is currently enabled and is not expected to be disabled in</td>
</tr>
<tr>
<td></td>
<td>the absence of administrative changes or changes in received protocol</td>
</tr>
<tr>
<td></td>
<td>information.</td>
</tr>
<tr>
<td></td>
<td>◦ Synchronization – The System considers this link to be IN_SYNC; i.e., it</td>
</tr>
<tr>
<td></td>
<td>has been allocated to the correct Link Aggregation Group, the group has</td>
</tr>
<tr>
<td></td>
<td>been associated with a compatible Aggregator, and the identity of the</td>
</tr>
<tr>
<td></td>
<td>Link Aggregation Group is consistent with the System ID and operational</td>
</tr>
<tr>
<td></td>
<td>Key information transmitted.</td>
</tr>
<tr>
<td></td>
<td>◦ Aggregation – The system considers this link to be aggregatable; i.e., a</td>
</tr>
<tr>
<td></td>
<td>potential candidate for aggregation.</td>
</tr>
<tr>
<td></td>
<td>◦ Long timeout – Periodic transmission of LACPDUs uses a slow transmission</td>
</tr>
<tr>
<td></td>
<td>rate.</td>
</tr>
<tr>
<td></td>
<td>◦ LACP-Activity – Activity control value with regard to this link.</td>
</tr>
<tr>
<td></td>
<td>(0: Passive; 1: Active)</td>
</tr>
</tbody>
</table>

```
Console#show lacp 1 neighbors
Port Channel 1 neighbors
  _____________________________________________________________
  Eth 1/1
  _____________________________________________________________
  Partner Admin System ID  : 32768, 00-00-00-00-00-00
  Partner Oper System ID   : 32768, 00-12-CF-61-24-2F
  Partner Admin Port Number: 1
  Partner Oper Port Number  : 1
  Port Admin Priority      : 32768
  Port Oper Priority       : 32768
  Admin Key                : 0
  Oper Key                 : 3
  Admin State:             defaulted, distributing, collecting, synchronization, long timeout, aggregation, long timeout, LACP-activity
  Oper State:              distributing, collecting, synchronization, aggregation, long timeout, LACP-activity

```

### Table 75: show lacp neighbors - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Admin System ID</td>
<td>LAG partner's system ID assigned by the user.</td>
</tr>
<tr>
<td>Partner Oper System ID</td>
<td>LAG partner's system ID assigned by the LACP protocol.</td>
</tr>
</tbody>
</table>
Table 75: show lACP neighbors - display description (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Admin Port Number</td>
<td>Current administrative value of the port number for the protocol Partner.</td>
</tr>
<tr>
<td>Partner Oper Port Number</td>
<td>Operational port number assigned to this aggregation port by the port’s protocol partner.</td>
</tr>
<tr>
<td>Port Admin Priority</td>
<td>Current administrative value of the port priority for the protocol partner.</td>
</tr>
<tr>
<td>Port Oper Priority</td>
<td>Priority value assigned to this aggregation port by the partner.</td>
</tr>
<tr>
<td>Admin Key</td>
<td>Current administrative value of the Key for the protocol partner.</td>
</tr>
<tr>
<td>Oper Key</td>
<td>Current operational value of the Key for the protocol partner.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Administrative values of the partner’s state parameters. (See preceding table.)</td>
</tr>
<tr>
<td>Oper State</td>
<td>Operational values of the partner’s state parameters. (See preceding table.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Console#show lACP sysid</th>
<th>Port Channel</th>
<th>System Priority</th>
<th>System MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>32768</td>
<td>00-30-F1-8F-2C-A7</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>32768</td>
<td>00-30-F1-8F-2C-A7</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>32768</td>
<td>00-30-F1-8F-2C-A7</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>32768</td>
<td>00-30-F1-8F-2C-A7</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>32768</td>
<td>00-30-F1-8F-2C-A7</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>32768</td>
<td>00-30-F1-8F-2C-A7</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>32768</td>
<td>00-30-F1-D4-73-A0</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>32768</td>
<td>00-30-F1-D4-73-A0</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>32768</td>
<td>00-30-F1-D4-73-A0</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>32768</td>
<td>00-30-F1-D4-73-A0</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>32768</td>
<td>00-30-F1-D4-73-A0</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>32768</td>
<td>00-30-F1-D4-73-A0</td>
</tr>
</tbody>
</table>

Table 76: show lACP sysid - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel group</td>
<td>A link aggregation group configured on this switch.</td>
</tr>
<tr>
<td>System Priority*</td>
<td>LACP system priority for this channel group.</td>
</tr>
<tr>
<td>System MAC Address*</td>
<td>System MAC address.</td>
</tr>
</tbody>
</table>

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

**show port-channel load-balance**

This command shows the load-distribution method used on aggregated links.

**Command Mode**
Privileged Exec
Example

```
Console#show port-channel load-balance
Trunk Load Balance Mode: Destination IP address
Console#
```
Power over Ethernet Commands

The commands in this group control the power that can be delivered to attached PoE devices through RJ-45 ports 1-24 on the EX-3524 and RJ-45 ports 1-48 on the EX-3548.

The switch’s power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Table 77: PoE Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>power inline compatible</td>
<td>Provides power to pre-standard PoE devices</td>
<td>GC</td>
</tr>
<tr>
<td>power mainpower maximum allocation</td>
<td>Sets the maximum power available to all switch ports</td>
<td>GC</td>
</tr>
<tr>
<td>power inline</td>
<td>Turns power on and off for specific ports</td>
<td>IC</td>
</tr>
<tr>
<td>power inline maximum allocation</td>
<td>Sets the maximum power available to specific switch ports</td>
<td>IC</td>
</tr>
<tr>
<td>power inline priority</td>
<td>Sets the priority for power supplied to specific ports</td>
<td>IC</td>
</tr>
<tr>
<td>power inline time-range</td>
<td>Binds a time-range to a port during which PoE is supplied</td>
<td>IC</td>
</tr>
<tr>
<td>show power inline status</td>
<td>Displays the current status of power management on specific ports or all ports</td>
<td>PE</td>
</tr>
<tr>
<td>show power inline time-range</td>
<td>Shows the time-range and current status for specific ports or for all ports</td>
<td>PE</td>
</tr>
</tbody>
</table>

**power inline compatible**

This command allows the switch to detect and provide power to powered devices that were designed prior to the IEEE 802.3af PoE standard. Use the no form to disable this feature.

**Syntax**

```
[no] power inline compatible
```

**Default Setting**

Disabled
Command Mode
Global Configuration

Command Usage
◆ The switch automatically detects attached PoE devices by periodically transmitting test voltages that over the Gigabit Ethernet copper-media ports. When an IEEE 802.3af or 802.3at compatible device is plugged into one of these ports, the powered device reflects the test voltage back to the switch, which may then turn on the power to this device. When the power inline compatible command is used, this switch can detect IEEE 802.3af or 802.3at compliant devices and the more recent 802.3af non-compliant devices that also reflect the test voltages back to the switch. It cannot detect other legacy devices that do not reflect back the test voltages.

◆ For legacy devices to be supported by this switch, they must be able to accept power over the data pairs connected to the RJ-45 ports.

Example

```
Console(config)#power inline compatible
Console(config)#end
Console#show power inline status
Unit: 1
Compatible mode: Enabled
Interface Admin Range Oper Power Used Power Priority
--------- -------- -------- ---- -------- -------- --------
Eth 1/1   Enabled --     Off 34200 mW 0 mW Low
Eth 1/2   Enabled --     Off 34200 mW 0 mW Low
Eth 1/3   Enabled --     Off 34200 mW 0 mW Low
Eth 1/4   Enabled --     Off 34200 mW 0 mW Low
Eth 1/5   Enabled --     Off 34200 mW 0 mW Low
Eth 1/6   Enabled --     Off 34200 mW 0 mW Low
Eth 1/7   Enabled --     Off 34200 mW 0 mW Low
Eth 1/8   Enabled --     Off 34200 mW 0 mW Low
Eth 1/9   Enabled --     Off 34200 mW 0 mW Low
Eth 1/10  Enabled --     Off 34200 mW 0 mW Low
Eth 1/11  Enabled --     Off 34200 mW 0 mW Low
Eth 1/12  Enabled --     Off 34200 mW 0 mW Low

power mainpower maximum allocation
```
This command defines a power budget for the switch (i.e., the power available to all switch ports). Use the no form to restore the default setting.

Syntax
```
power mainpower maximum allocation watts

watts - The power budget for the switch.
(EX-3524: 50000-390000 milliwatts
EX-3548: 50000-779000 milliwatts)
```
Default Setting
EX-3524: 390000 milliwatts
EX-3548: 779000 milliwatts

Command Mode
Global Configuration

Command Usage
◆ Setting a maximum power budget for the switch enables power to be centrally managed, preventing overload conditions at the power source.
◆ If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.

Example
```console
Console(config)#power mainpower maximum allocation 180
Console(config)#
```

Related Commands
power inline priority (421)

power inline
This command instructs the switch to automatically detect if a PoE-compliant device is connected to the specified port, and turn power on or off accordingly. Use the no form to turn off power for a port, or the no form with the time-range keyword to remove the time range settings.

Syntax
```
power inline [time-range time-range-name]
no power inline [time-range]
```

*time-range-name* - Name of a time-range during which PoE is supplied to the attached device. (Range: 1-32 characters)

Default Setting
Detection is enabled for PoE-compliant devices.

Command Mode
Interface Configuration (Ethernet ports 1-24/48)

Command Usage
◆ The switch only provides power to the Gigabit Ethernet copper-media ports.
◆ When detection is enabled for PoE-compliant devices, power is automatically supplied when a device is detected on the port, providing that the power
demanded does not exceed the port’s power budget or the switch’s power budget.

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#power inline
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#no power inline
Console(config-if)#
```

**Related Commands**

time-range (155)

**power inline maximum allocation**

This command limits the power allocated to specific ports. Use the `no` form to restore the default setting.

**Syntax**

```plaintext
power inline maximum allocation milliwatts
no power inline maximum allocation
```

- `milliwatts` - The maximum power budget for the port.
  (Range: 3000 - 34200 milliwatts)

**Default Setting**

34200 milliwatts

**Command Mode**

Interface Configuration (Ethernet ports 1-24/48)

**Command Usage**

- For the EX-3524, the total PoE power delivered by all ports cannot exceed the maximum power budget of 390W. For the EX-3548, the total PoE power delivered by all ports cannot exceed the maximum power budget of 779W. All the RJ-45 ports support both the IEEE 802.3af and IEEE 802.3at standards. The maximum number of ports which can supply power simultaneously at the specified levels are shown in the following table.

<table>
<thead>
<tr>
<th>Switch</th>
<th>34.2W (802.3at)</th>
<th>15.4W (802.3af)</th>
<th>7.5W (802.3af)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX-3524</td>
<td>11</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>EX-3524</td>
<td>22</td>
<td>48</td>
<td>48</td>
</tr>
</tbody>
</table>

- If a device is connected to a switch port and the switch detects that it requires more than the maximum power allocated to the port or to the overall switch, no power is supplied to the device (i.e., port power remains off).
Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline maximum allocation 8000
Console(config-if)#
```

**power inline priority**  This command sets the power priority for specific ports. Use the no form to restore the default setting.

**Syntax**

```
power inline priority priority
no power inline priority
```

- **priority** - The power priority for the port.
  Options: 1 (critical), 2 (high), or 3 (low)

**Default Setting**

3 (low)

**Command Mode**

Interface Configuration

**Command Usage**

- If the power demand from devices connected to the switch exceeds the power budget setting as determined during bootup, the switch uses port power priority settings to control the supplied power. For example:

  - A device connected to a low-priority port that causes the switch to exceed its budget is not supplied power.

  - If a device is connected to a critical or high-priority port and would cause the switch to exceed its power budget as determined during bootup, power is provided to the port only if the switch can drop power to one or more lower-priority ports and thereby remain within its overall budget.

  - If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port regardless of its priority setting.
If priority is not set for any ports, and PoE consumption exceeds the maximum power provided by the switch, power is shut down in the following sequence:

**Table 79: PoE Shut Down Sequence**

<table>
<thead>
<tr>
<th>Switch</th>
<th>PoE Port Shut Down Sequence</th>
</tr>
</thead>
</table>
| EX-3524 | PSE#1: 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1,  
PSE#2: 24, 23, 22, 21, 20, 19, 18, 17, 16, 15, 14, 13 |
| EX-3548 | PSE#1: 1,3,2,5,4,7,6,9,8,11,10,  
PSE#2: 13,12,15,14,17,16 19,18,21,20,23,22,25,  
PSE#3: 24,27,26,29,28,31,30,33,32,35,34,37,  
PSE#4: 36,39,38,41,40,43,42,45,44,47,46 |

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#power inline priority 2
Console(config-if)#
```

**power inline time-range**

This command binds a time-range to a port during which PoE is supplied to the attached device. Use the **no** form to remove this binding.

**Syntax**

```
power inline time-range time-range-name  
no power inline time-range  
```

* `time-range-name` - Name of the time range. (Range: 1-32 characters)

**Default Setting**

None

**Command Mode**

Interface Configuration

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#power inline time-range rd
Console(config-if)#
```

**Related Commands**

`time-range (155)`
**show power inline status**  
This command displays the current power status for all ports or for specific ports.

**Syntax**

```
show power inline status [interface]
```

*interface*

- **ethernet**

  *unit* - Unit identifier. (Range: 1)
  
  *port* - Port number. (Range: 1-24/48)

**Command Mode**

Privileged Exec

**Example**

```
Console#show power inline status
Unit: 1
Compatible mode : Enabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Time</th>
<th>Max</th>
<th>Used</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>Enabled</td>
<td>Off</td>
<td>34200 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>Enabled</td>
<td>Off</td>
<td>34200 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/3</td>
<td>Enabled</td>
<td>On</td>
<td>34200 mW</td>
<td>7505 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/4</td>
<td>Enabled</td>
<td>Off</td>
<td>34200 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/5</td>
<td>Enabled</td>
<td>Off</td>
<td>34200 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/6</td>
<td>Enabled</td>
<td>Off</td>
<td>34200 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/7</td>
<td>Enabled</td>
<td>On</td>
<td>15400 mW</td>
<td>8597 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/8</td>
<td>Enabled</td>
<td>Off</td>
<td>15400 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/9</td>
<td>Enabled</td>
<td>Off</td>
<td>15400 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/10</td>
<td>Enabled</td>
<td>Off</td>
<td>15400 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/11</td>
<td>Enabled</td>
<td>Off</td>
<td>15400 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
<tr>
<td>Eth 1/12</td>
<td>Enabled</td>
<td>Off</td>
<td>15400 mW</td>
<td>0 mW</td>
<td>Low</td>
</tr>
</tbody>
</table>
```

**Table 80: show power inline status - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The power mode set on the port (see power inline)</td>
</tr>
<tr>
<td>Time Range</td>
<td>Time during which power is supplied</td>
</tr>
<tr>
<td>Oper</td>
<td>The current operating power status (displays on or off)</td>
</tr>
<tr>
<td>Power (mWatt)</td>
<td>The maximum power allocated to this port (see power inline maximum allocation)</td>
</tr>
<tr>
<td>Power (used)</td>
<td>The current power consumption on the port in milliwatts</td>
</tr>
<tr>
<td>Priority</td>
<td>The port’s power priority setting (see power inline priority)</td>
</tr>
</tbody>
</table>
**show power inline time-range**

This command displays the time-range and current status for specific ports or for all ports.

**Syntax**

```
show power inline time-range time-range-name [interface]
```

- **time-range-name** - Name of the time range. (Range: 1-32 characters)
- **interface**
  - **ethernet**
    - **unit** - Unit identifier. (Range: 1)
    - **port** - Port number. (Range: 1-24/48)

**Command Mode**

Privileged Exec

**Example**

```
Console#show power inline time-range ethernet 1/5
Interface Time Range Name Status
--------- ---------------- --------
Eth 1/ 5  r&d              Inactive
Console#
```

**Related Commands**

- **power inline (419)**

**show power mainpower**

Use this command to display the current power status for the switch.

**Command Mode**

Privileged Exec

**Example**

This example shows the maximum available PoE power and maximum allocated PoE power for the EX-3424.

```
Console#show power mainpower
Unit 1 PoE Status
PoE Maximum Available Power  : 390.0 Watts
PoE Maximum Allocation Power : 390.0 Watts
System Operation Status     : On
PoE Power Consumption        : 0.0 Watts
Software Version             : Version 0068 (Hex), Build 00 (Hex)
Console#
```
Port Mirroring Commands

Data can be mirrored from a local port on the same switch or from a remote port on another switch for analysis at the target port using software monitoring tools or a hardware probe. This switch supports the following mirroring modes.

### Table 81: Port Mirroring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Port Mirroring</td>
<td>Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port</td>
</tr>
<tr>
<td>RSPAN Mirroring</td>
<td>Mirrors data from remote switches over a dedicated VLAN</td>
</tr>
</tbody>
</table>

### Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

### Table 82: Mirror Port Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>port monitor</td>
<td>Configures a mirror session</td>
<td>IC</td>
</tr>
<tr>
<td>show port monitor</td>
<td>Shows the configuration for a mirror port</td>
<td>PE</td>
</tr>
</tbody>
</table>

**port monitor** This command configures a mirror session. Use the **no** form to clear a mirror session.

**Syntax**

```
port monitor {interface [rx | tx | both] | vlan vlan-id | mac-address mac-address | access-list acl-name}
```

```
no port monitor {interface | vlan vlan-id | mac-address mac-address | access-list acl-name}
```

```
interface
    ethernet unit/port (source port)
    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)
```

```
rx - Mirror received packets.
```

```
tx - Mirror transmitted packets.
```
**both** - Mirror both received and transmitted packets.

vlan-id - VLAN ID (Range: 1-4094)

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxxx.

acl-name – Name of the ACL. (Maximum length: 32 characters, no spaces or other special characters)

**Default Setting**
- No mirror session is defined.
- When enabled for an interface, default mirroring is for both received and transmitted packets.
- When enabled for a VLAN or a MAC address, mirroring is restricted to received packets.

**Command Mode**
Interface Configuration (Ethernet, destination port)

**Command Usage**
- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.

- Set the destination port by specifying an Ethernet interface with the `interface` configuration command, and then use the `port monitor` command to specify the source of the traffic to mirror. Note that the destination port cannot be a trunk or trunk member port.

- When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.

- When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirror VLAN.

- When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.

- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to the target port specified for port mirroring.

- When mirroring VLAN traffic or packets based on a source MAC address, the target port cannot be set to the same target port as that used for basic port mirroring.
Chapter 13 | Port Mirroring Commands

Local Port Mirroring Commands

◆ Spanning Tree BPDU packets are not mirrored to the target port.

◆ You can create multiple mirror sessions which can share the same destination port, or mirror traffic to different destination ports.

◆ The destination port cannot be a trunk or trunk member port.

◆ RSPAN and 802.1X are mutual exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source ports and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally. Also, RSPAN uplink ports cannot be configured to use IEEE802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it.

◆ ACL-based mirroring is only used for ingress traffic. To mirror an ACL, follow these steps:

1. Use the **access-list** command to add an ACL.
2. Use the **access-group** command to add a mirrored port to access control list.
3. Use the **port monitor access-list** command to specify the destination port to which traffic matching the ACL will be mirrored.

**Example**
The following example configures the switch to mirror all packets from port 6 to 11:

```bash
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

This example configures port 2 to monitor packets matching the MAC address 00-12-CF-XX-XX-XX received by port 1:

```bash
Console(config)#access-list mac m1
Console(config-mac-acl)#permit 00-12-cf-00-00-00 ff-ff-ff-00-00-00 any
Console(config-mac-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#mac access-group m1 in
Console(config-if)#interface ethernet 1/2
Console(config-if)#port monitor access-list m1
Console(config-if)#
```
show port monitor  This command displays mirror information.

Syntax

    show port monitor [interface | vlan vlan-id | mac-address mac-address]

    interface - ethernet unit/port (source port)
        unit - Unit identifier. (Range: 1)
        port - Port number. (Range: 1-28/52)
    vlan-id - VLAN ID (Range: 1-4094)
    mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxxx.

Default Setting
Shows all sessions.

Command Mode
Privileged Exec

Command Usage
This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example
The following shows mirroring configured from port 6 to port 11:

```plaintext
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
    Destination Port (listen port): Eth1/11
    Source Port (monitored port)  : Eth1/ 6
    Mode                         : RX/TX
Console#
```

RSPAN Mirroring Commands

Remote Switched Port Analyzer (RSPAN) allows you to mirror traffic from remote switches for analysis on a local destination port.

Table 83: RSPAN Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan rspan</td>
<td>Creates a VLAN dedicated to carrying RSPAN traffic</td>
<td>VC</td>
</tr>
<tr>
<td>rspan source</td>
<td>Specifies the source port and traffic type to be mirrored</td>
<td>GC</td>
</tr>
</tbody>
</table>
Configuration Guidelines

Take the following steps to configure an RSPAN session:

1. Use the `vlan rspan` command to configure a VLAN to use for RSPAN. (Default VLAN 1 is prohibited.)

2. Use the `rspan source` command to specify the interfaces and the traffic type (RX, TX or both) to be monitored.

3. Use the `rspan destination` command to specify the destination port for the traffic mirrored by an RSPAN session.

4. Use the `rspan remote vlan` command to specify the VLAN to be used for an RSPAN session, to specify the switch's role as a source, intermediate relay, or destination of the mirrored traffic, and to configure the uplink ports designated to carry this traffic.

RSPAN Limitations

The following limitations apply to the use of RSPAN on this switch:

- **RSPAN Ports** – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.

  Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink or destination port – access ports are not allowed (see `switchport mode`).

- **Local/Remote Mirror** – The destination of a local mirror session (created with the `port monitor` command) cannot be used as the destination for RSPAN traffic.

  Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled, then no session can be configured for RSPAN.
◆ **Spanning Tree** – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.

MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.

◆ **IEEE 802.1X** – RSPAN and 802.1X are mutually exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

RSPAN uplink ports cannot be configured to use IEEE 802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it

◆ **Port Security** – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

---

**rspan source**

Use this command to specify the source port and traffic type to be mirrored remotely. Use the `no` form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

**Syntax**

```
[no] rspan session session-id source interface interface-list [rx | tx | both]
```

- **session-id** – A number identifying this RSPAN session. (Range: 1)
  - Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled with the `port monitor` command, then no session can be configured for RSPAN.
  - `interface-list` – One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

```
ethernet unit/port
```

- **unit** - Unit identifier. (Range: 1)
- **port** - Port number. (Range: 1-28/52)

- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

**Default Setting**

Both TX and RX traffic is mirrored
Chapter 13 | Port Mirroring Commands
RSPAN Mirroring Commands

Command Mode
Global Configuration

Command Usage
◆ One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
◆ Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.
◆ The source port and destination port cannot be configured on the same switch.

Example
The following example configures the switch to mirror received packets from port 2 and 3:

```
Console(config)#rspan session 1 source interface ethernet 1/2
Console(config)#rspan session 1 source interface ethernet 1/3
Console(config)#
```

```
rspan destination
```
Use this command to specify the destination port to monitor the mirrored traffic. Use the `no` form to disable RSPAN on the specified port.

Syntax
```
rspan session session-id destination interface interface [tagged | untagged]
no rspan session session-id destination interface interface
```

- `session-id` – A number identifying this RSPAN session. (Range: 1)

  Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled with the `port monitor` command, then no session can be configured for RSPAN.

- `interface` - `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)

- `tagged` - Traffic exiting the destination port carries the RSPAN VLAN tag.
- `untagged` - Traffic exiting the destination port is untagged.

Default Setting
Traffic exiting the destination port is untagged.

Command Mode
Global Configuration
Command Usage
◆ Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.

◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN destination port – access ports are not allowed (see switchport mode).

◆ Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.

◆ The source port and destination port cannot be configured on the same switch.

◆ A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

Example
The following example configures port 4 to receive mirrored RSPAN traffic:

```
Console(config)#rspan session 1 destination interface ethernet 1/2
```

rspan remote vlan
Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the no form to disable the RSPAN on the specified VLAN.

Syntax

```
[no] rspan session session-id remote vlan vlan-id
{source | intermediate | destination} uplink interface
```

session-id – A number identifying this RSPAN session. (Range: 1)

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then no session can be configured for RSPAN.

vlan-id - ID of configured RSPAN VLAN. (Range: 1-4094)

Use the vlan rspan command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

source - Specifies this device as the source of remotely mirrored traffic.

intermediate - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

destination - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

uplink - A port configured to receive or transmit remotely mirrored traffic.
interface - **ethernet unit/port**

**ethernet unit/port**

  *unit* - Unit identifier. (Range: 1)
  *port* - Port number. (Range: 1-28/52)

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink port – access ports are not allowed (see switchport mode).

◆ Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.

◆ Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the switchport allowed vlan command. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the show vlan command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

**Example**

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

**no rspan session** Use this command to delete a configured RSPAN session.

**Syntax**

```
no rspan session session-id
```

  *session-id* – A number identifying this RSPAN session. (Range: 1)

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then no session can be configured for RSPAN.

**Command Mode**

Global Configuration
Command Usage
The **no rspan session** command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the `vlan` command).

Example
```
Console(config)#no rspan session 1
Console(config)#
```

**show rspan**  Use this command to displays the configuration settings for an RSPAN session.

Syntax

```
show rspan session [session-id]
```

- **session-id** – A number identifying this RSPAN session. (Range: 1)

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled with the `port monitor` command, then no session can be configured for RSPAN.

Command Mode
Privileged Exec

Example
```
Console#show rspan session
RSPAN Session ID : 1
Source Ports (mirrored ports) : None
   RX Only : None
   TX Only : None
   BOTH : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode : Untagged
Switch Role : Destination
RSPAN VLAN : 2
RSPAN Uplink Ports : Eth 1/3
Operation Status : Up
Console#
```
Congestion Control Commands

The switch can set the maximum upload or download data transfer rate for any port. It can control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Table 84: Congestion Control Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limiting</td>
<td>Sets the input and output rate limits for a port.</td>
</tr>
<tr>
<td>Storm Control</td>
<td>Sets the traffic storm threshold for each port.</td>
</tr>
<tr>
<td>Automatic Traffic Control</td>
<td>Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.</td>
</tr>
</tbody>
</table>

Rate Limit Commands

Rate limit commands allow the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 85: Rate Limit Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit</td>
<td>Configures the maximum input or output rate for an interface</td>
<td>IC</td>
</tr>
</tbody>
</table>
**rate-limit**  This command defines the rate limit for a specific interface. Use this command without specifying a rate to enable rate limiting. Use the **no** form to disable rate limiting.

**Syntax**

```
rate-limit {input | output} [rate]
no rate-limit {input | output}
```

- **input** – Input rate for specified interface
- **output** – Output rate for specified interface
- **rate** – Maximum value in kbps. (Range: 64-1000000 kbps)

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

**Related Command**
*show interfaces switchport (389)*
Storm Control Commands

Storm control commands can be used to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Table 86: Rate Limit Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport packet-rate*</td>
<td>Configures broadcast, multicast, and unknown unicast storm control thresholds</td>
<td>IC</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays the administrative and operational status of an interface</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

* Enabling hardware-level storm control with this command on a port will disable software-level automatic storm control on the same port if configured by the auto-traffic-control command.

**switchport packet-rate**

This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

**Syntax**

```
switchport (broadcast | multicast | unknown-unicast) packet-rate rate
no switchport (broadcast | multicast | unknown-unicast)
```

- **broadcast** - Specifies storm control for broadcast traffic.
- **multicast** - Specifies storm control for multicast traffic.
- **unknown-unicast** - Specifies storm control for unknown unicast traffic.
- **rate** - Threshold level as a rate. (Range: 500-1488100 pps)

**Default Setting**

- Broadcast Storm Control: Enabled, 500 pps
- Multicast Storm Control: Disabled
- Unknown Unicast Storm Control: Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
Traffic storms can be controlled at the hardware level using this command or at the software level using the `auto-traffic-control` command. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.

The rate limits set by this command are also used by automatic storm control when the control response is set to rate limiting by the `auto-traffic-control action` command.

Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

**Example**
The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
```

**RELATED COMMANDS**
show interfaces switchport (389)

---

**Automatic Traffic Control Commands**

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

**Table 87: ATC Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threshold Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>auto-traffic-control apply-timer</code></td>
<td>Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold</td>
<td>GC</td>
</tr>
<tr>
<td><code>auto-traffic-control release-timer</code></td>
<td>Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold</td>
<td>GC</td>
</tr>
<tr>
<td><code>auto-traffic-control action</code></td>
<td>Enables automatic traffic control for broadcast or multicast storms</td>
<td>IC (Port)</td>
</tr>
<tr>
<td><code>auto-traffic-control alarm-clear-threshold</code></td>
<td>Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent</td>
<td>IC (Port)</td>
</tr>
</tbody>
</table>
### Table 87: ATC Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-traffic-control alarm-fire-threshold</td>
<td>Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires</td>
<td>IC (Port)</td>
</tr>
<tr>
<td>auto-traffic-control auto-control-release</td>
<td>Automatically releases a control response</td>
<td>IC (Port)</td>
</tr>
<tr>
<td>auto-traffic-control control-release</td>
<td>Manually releases a control response</td>
<td>PE</td>
</tr>
</tbody>
</table>

#### SNMP Trap Commands

- `snmp-server enable port-traps atc broadcast-alarm-clear` Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered | IC (Port) |
- `snmp-server enable port-traps atc broadcast-alarm-fire` Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control | IC (Port) |
- `snmp-server enable port-traps atc broadcast-control-apply` Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires | IC (Port) |
- `snmp-server enable port-traps atc broadcast-control-release` Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires | IC (Port) |
- `snmp-server enable port-traps atc multicast-alarm-clear` Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered | IC (Port) |
- `snmp-server enable port-traps atc multicast-alarm-fire` Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control | IC (Port) |
- `snmp-server enable port-traps atc multicast-control-apply` Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires | IC (Port) |
- `snmp-server enable port-traps atc multicast-control-release` Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires | IC (Port) |

#### ATC Display Commands

- `show auto-traffic-control` Shows global configuration settings for automatic storm control | PE |
- `show auto-traffic-control interface` Shows interface configuration settings and storm control status for the specified port | PE |

---

* Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the `switchport packet-rate` command.
Usage Guidelines
ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Figure 1: Storm Control by Limiting the Traffic Rate

The key elements of this diagram are described below:

- **Alarm Fire Threshold** – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.

- When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.

- **Alarm Clear Threshold** – The lower threshold beneath which a control response can be automatically terminated after the release timer expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.

- When traffic falls below the alarm clear threshold after the release timer expires, traffic control (for rate limiting) will be stopped and a Traffic Control Release Trap sent and logged. Note that if the control action has shut down a port, it can only be manually re-enabled using the `auto-traffic-control control-release` command.

- The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.
Figure 2: Storm Control by Shutting Down a Port

The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

**Functional Limitations**
Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the `switchport packet-rate` command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

**Threshold Commands**

- `auto-traffic-control`
- `apply-timer`

This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the `no` form to restore the default setting.

**Syntax**

```
auto-traffic-control {broadcast | multicast} apply-timer seconds

no auto-traffic-control {broadcast | multicast} apply-timer
```

- `broadcast` - Specifies automatic storm control for broadcast traffic.
- `multicast` - Specifies automatic storm control for multicast traffic.
- `seconds` - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 5-300 seconds)

**Default Setting**

300 seconds

**Command Mode**

Global Configuration
**Command Usage**

After the apply timer expires, a control action may be triggered as specified by the `auto-traffic-control action` command and a trap message sent as specified by the `snmp-server enable port-traps atc broadcast-control-apply` command or `snmp-server enable port-traps atc multicast-control-apply` command.

**Example**

This example sets the apply timer to 200 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

**auto-traffic-control release-timer**

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the `no` form to restore the default setting.

**Syntax**

```
auto-traffic-control {broadcast | multicast} release-timer seconds
no auto-traffic-control {broadcast | multicast} release-timer
```

- `broadcast` - Specifies automatic storm control for broadcast traffic.
- `multicast` - Specifies automatic storm control for multicast traffic.
- `seconds` - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold. (Range: 5-900 seconds)

**Default Setting**

900 seconds

**Command Mode**

Global Configuration

**Command Usage**

This command sets the delay after which the control response can be terminated. The `auto-traffic-control auto-control-release` command must be used to enable or disable the automatic release of a control response of rate-limiting. To re-enable a port which has been shut down by automatic traffic control, you must manually re-enable the port using the `auto-traffic-control control-release` command.

**Example**

This example sets the release timer to 800 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```
auto-traffic-control  This command enables automatic traffic control for broadcast or multicast storms. Use the no form to disable this feature.

Syntax

[no] auto-traffic-control {broadcast | multicast}

broadcast - Specifies automatic storm control for broadcast traffic.
multicast - Specifies automatic storm control for multicast traffic.

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet)

Command Usage
◆ Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.

◆ Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

Example
This example enables automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control action  This command sets the control action to limit ingress traffic or shut down the offending port. Use the no form to restore the default setting.

Syntax

auto-traffic-control {broadcast | multicast} action {rate-control | shutdown}

no auto-traffic-control {broadcast | multicast} action

broadcast - Specifies automatic storm control for broadcast traffic.
multicast - Specifies automatic storm control for multicast traffic.
rate-control - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the auto-traffic-control alarm-clear-threshold command.
Chapter 14 | Congestion Control Commands
Automatic Traffic Control Commands

**shutdown** - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

**Default Setting**
- rate-control

**Command Mode**
- Interface Configuration (Ethernet)

**Command Usage**
- When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.
- When the control response is set to rate limiting by this command, the rate limits are determined by the `auto-traffic-control alarm-clear-threshold` command.
- If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.
- If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the `auto-traffic-control control-release` command.

**Example**
This example sets the control response for broadcast traffic on port 1.

```bash
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

**auto-traffic-control**

**alarm-clear-threshold**
- This command sets the lower threshold for ingress traffic beneath which a control response for rate limiting will be released after the Release Timer expires, if so configured by the `auto-traffic-control auto-control-release` command. Use the `no` form to restore the default setting.

**Syntax**

```bash
auto-traffic-control (broadcast | multicast) alarm-clear-threshold threshold
no auto-traffic-control (broadcast | multicast) alarm-clear-threshold
```
- `broadcast` - Specifies automatic storm control for broadcast traffic.
- `multicast` - Specifies automatic storm control for multicast traffic.
- `threshold` - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second)
**Chapter 14 | Congestion Control Commands**

**Automatic Traffic Control Commands**

**Default Setting**
250 kilo-packets per second

**Command Mode**
Interface Configuration (Ethernet)

**Command Usage**

- Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the `snmp-server enable port-traps atc broadcast-alarm-clear` command or `snmp-server enable port-traps atc multicast-alarm-clear` command.

- If rate limiting has been configured as a control response, it will be discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the `auto-traffic-control control-release` command.

**Example**
This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

**auto-traffic-control alarm-fire-threshold**

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

**Syntax**

```
auto-traffic-control {broadcast | multicast} alarm-fire-threshold threshold
no auto-traffic-control {broadcast | multicast} alarm-fire-threshold

broadcast - Specifies automatic storm control for broadcast traffic.
multicast - Specifies automatic storm control for multicast traffic.
threshold - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. (Range: 1-255 kilo-packets per second)
```

**Default Setting**
250 kilo-packets per second

**Command Mode**
Interface Configuration (Ethernet)
Command Usage
◆ Once the upper threshold is exceeded, a trap message may be sent if configured by the `snmp-server enable port-traps atc broadcast-alarm-fire` command or `snmp-server enable port-traps atc multicast-alarm-fire` command.

◆ After the upper threshold is exceeded, the control timer must first expire as configured by the `auto-traffic-control apply-timer` command before a control response is triggered if configured by the `auto-traffic-control action` command.

Example
This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

**auto-traffic-control auto-control-release**
This command automatically releases a control response of rate-limiting after the time specified in the `auto-traffic-control release-timer` command has expired.

Syntax
```
auto-traffic-control {broadcast | multicast} auto-control-release
```
- `broadcast` - Specifies automatic storm control for broadcast traffic.
- `multicast` - Specifies automatic storm control for multicast traffic.

Command Mode
Interface Configuration (Ethernet)

Command Usage
◆ This command can be used to automatically stop a control response of rate-limiting after the specified action has been triggered and the release timer has expired.

◆ To release a control response which has shut down a port after the specified action has been triggered and the release timer has expired, use the `auto-traffic-control control-release` command.

Example
```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```
**auto-traffic-control control-release**
This command manually releases a control response.

**Syntax**
```
auto-traffic-control {broadcast | multicast} control-release
interface interface

broadcast - Specifies automatic storm control for broadcast traffic.
multicast - Specifies automatic storm control for multicast traffic.

interface

ethernet unit/port-list

unit - Unit identifier. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-28/52)
```

**Command Mode**
Privileged Exec

**Command Usage**
This command can be used to manually stop a control response of rate-limiting or port shutdown any time after the specified action has been triggered.

**Example**
```
Console#auto-traffic-control broadcast control-release interface ethernet 1/1
Console#
```

**SNMP Trap Commands**

**snmp-server enable port-traps atc broadcast-alarm-clear**
This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the `no` form to disable this trap.

**Syntax**
```
[no] snmp-server enable port-traps atc broadcast-alarm-clear
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet)
Example

```plaintext
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)#
```

Related Commands
- auto-traffic-control action (443)
- auto-traffic-control alarm-clear-threshold (444)
- snmp-server enable port-traps atc broadcast-alarm-fire

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the `no` form to disable this trap.

Syntax
```
[no] snmp-server enable port-traps atc broadcast-alarm-fire
```

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet)

Example

```plaintext
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

Related Commands
- auto-traffic-control alarm-fire-threshold (445)
- snmp-server enable port-traps atc broadcast-control-apply

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the `no` form to disable this trap.

Syntax
```
[no] snmp-server enable port-traps atc broadcast-control-apply
```

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet)
Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply
Console(config-if)#
```

Related Commands
auto-traffic-control alarm-fire-threshold (445)
auto-traffic-control apply-timer (441)

```
**snmp-server enable port-traps atc broadcast-control-release**

This command sends a trap when broadcast traffic falls beneath the lower
threshold after a storm control response has been triggered and the release timer
expires. Use the `no` form to disable this trap.

**Syntax**

```
[no] snmp-server enable port-traps atc broadcast-control-release
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet)

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-release
Console(config-if)#
```

**Related Commands**

auto-traffic-control alarm-clear-threshold (444)
auto-traffic-control action (443)
auto-traffic-control release-timer (442)

```
**snmp-server enable port-traps atc multicast-alarm-clear**

This command sends a trap when multicast traffic falls beneath the lower threshold
after a storm control response has been triggered. Use the `no` form to disable this
trap.

**Syntax**

```
[no] snmp-server enable port-traps atc multicast-alarm-clear
```

**Default Setting**

Disabled
Chapter 14 | Congestion Control Commands

Automatic Traffic Control Commands

Command Mode
Interface Configuration (Ethernet)

Example

```console
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

Related Commands

- `auto-traffic-control action (443)`
- `auto-traffic-control alarm-clear-threshold (444)`

### `snmp-server enable port-traps atc multicast-alarm-fire`

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the `no` form to disable this trap.

**Syntax**

```
[no] snmp-server enable port-traps atc multicast-alarm-fire
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet)

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

**Related Commands**

- `auto-traffic-control alarm-fire-threshold (445)`

### `snmp-server enable port-traps atc multicast-control-apply`

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the `no` form to disable this trap.

**Syntax**

```
[no] snmp-server enable port-traps atc multicast-control-apply
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet)
Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-apply
Console(config-if)#
```

Related Commands

- `auto-traffic-control alarm-fire-threshold (445)`
- `auto-traffic-control apply-timer (441)`

**snmp-server enable port-traps atc multicast-control-release**

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the `no` form to disable this trap.

**Syntax**

```
[no] snmp-server enable port-traps atc multicast-control-release
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet)

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-release
Console(config-if)#
```

Related Commands

- `auto-traffic-control alarm-clear-threshold (444)`
- `auto-traffic-control action (443)`
- `auto-traffic-control release-timer (442)`

**ATC Display Commands**

**show auto-traffic-control**

This command shows global configuration settings for automatic storm control.

**Command Mode**

Privileged Exec

**Example**

```
Console#show auto-traffic-control
Storm-control: Broadcast
Apply-timer (sec) : 300
```
show auto-traffic-control interface

This command shows interface configuration settings and storm control status for the specified port.

Syntax

```
show auto-traffic-control interface [interface]
```

*interface*

- ethernet unit/port
  - *unit* - Unit identifier. (Range: 1)
  - *port* - Port number. (Range: 1-28/52)

Command Mode

Privileged Exec

Example

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
---------------------------------------------------------------
Storm Control: Broadcast Multicast
State: Disabled Disabled
Action: rate-control rate-control
Auto Release Control: Disabled Disabled
Alarm Fire Threshold(Kpps): 250 250
Alarm Clear Threshold(Kpps):250 250
Trap Storm Fire: Disabled Disabled
Trap Storm Clear: Disabled Disabled
Trap Traffic Apply: Disabled Disabled
Trap Traffic Release: Disabled Disabled
```

Console#
Loopback Detection Commands

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Table 88: Loopback Detection Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback-detection</td>
<td>Enables loopback detection globally on the switch or on a specified interface</td>
<td>GC, IC</td>
</tr>
<tr>
<td>loopback-detection action</td>
<td>Specifies the response to take for a detected loopback condition</td>
<td>GC</td>
</tr>
<tr>
<td>loopback-detection recover-time</td>
<td>Specifies the interval to wait before releasing an interface from shutdown state</td>
<td>GC</td>
</tr>
<tr>
<td>loopback-detection transmit-interval</td>
<td>Specifies the interval at which to transmit loopback detection control frames</td>
<td>GC</td>
</tr>
<tr>
<td>loopback detection trap</td>
<td>Configures the switch to send a trap when a loopback condition is detected or the switch recover from a loopback</td>
<td>GC</td>
</tr>
<tr>
<td>loopback-detection release</td>
<td>Manually releases all interfaces currently shut down by the loopback detection feature</td>
<td>PE</td>
</tr>
<tr>
<td>show loopback-detection</td>
<td>Shows loopback detection configuration settings for the switch or for a specified interface</td>
<td>PE</td>
</tr>
</tbody>
</table>

Usage Guidelines

◆ The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.

◆ General loopback detection provided by the commands described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.

◆ When a loopback event is detected on an interface or when a interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.

◆ Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.
**loopback-detection** This command enables loopback detection globally on the switch or on a specified interface. Use the no form to disable loopback detection.

**Syntax**
```
[no] loopback-detection
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
Loopback detection must be enabled globally for the switch by this command and enabled for a specific interface for this function to take effect.

**Example**
This example enables general loopback detection on the switch, disables loopback detection provided for the spanning tree protocol on port 1, and then enables general loopback detection for that port.

```
Console(config)#loopback-detection
Console(config)#interface ethernet 1/1
Console(config-if)#no spanning-tree loopback-detection
Console(config-if)#loopback-detection
Console(config)#
```

**loopback-detection action** This command specifies the protective action the switch takes when a loopback condition is detected. Use the no form to restore the default setting.

**Syntax**
```
loopback-detection action {block | none | shutdown}
no loopback-detection action
```

**Default Setting**
Shut down

**Command Mode**
Global Configuration
Command Usage

◆ When the response to a detected loopback condition is set to block user traffic, loopback detection control frames may untagged or tagged depending on the port's VLAN membership type.

◆ When the response to a detected loopback condition is set to block user traffic, ingress filtering for the port is enabled automatically if not already enabled by the switchport ingress-filtering command. The port's original setting for ingress filtering will be restored when loopback detection is disabled.

◆ When a port receives a control frame sent by itself, this means that the port is in looped state, and the VLAN in the frame payload is also in looped state with the wrong VLAN tag. The looped port therefore be shut down.

◆ Use the loopback-detection recover-time command to set the time to wait before re-enabling an interface shut down by the loopback detection process.

◆ When the loopback detection response is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

Example

This example sets the loopback detection mode to block user traffic.

```
Console(config)#loopback-detection action block
Console(config)#
```

loopback-detection recover-time

This command specifies the interval to wait before the switch automatically releases an interface from shutdown state. Use the no form to restore the default setting.

Syntax

```
loopback-detection recover-time seconds
no loopback-detection recover-time
```

seconds - Recovery time from shutdown state. (Range: 60-1,000,000 seconds, or 0 to disable automatic recovery)

Default Setting

60 seconds

Command Mode

Global Configuration
**Command Usage**

- When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

- If the recovery time is set to zero, all ports placed in shutdown state can be restored to operation using the `loopback-detection release` command. To restore a specific port, use the `no shutdown` command.

**Example**

```
Console(config)#loopback-detection recover-time 120
Console(config-if)#
```

---

**loopback-detection transmit-interval**

This command specifies the interval at which to transmit loopback detection control frames. Use the `no` form to restore the default setting.

**Syntax**

```
loopback-detection transmit-interval seconds
no loopback-detection transmit-interval
```

- `seconds` - The transmission interval for loopback detection control frames.
  (Range: 1-32767 seconds)

**Default Setting**

10 seconds

**Command Mode**

Global Configuration

**Example**

```
Console(config)#loopback-detection transmit-interval 60
Console(config)#
```

---

**loopback-detection trap**

This command sends a trap when a loopback condition is detected, or when the switch recovers from a loopback condition. Use the `no` form to restore the default state.

**Syntax**

```
loopback-detection trap [both | detect | none | recover]
no loopback-detection trap
```

- `both` - Sends an SNMP trap message when a loopback condition is detected, or when the switch recovers from a loopback condition.
**detect** - Sends an SNMP trap message when a loopback condition is detected.

**none** - Does not send an SNMP trap for loopback detection or recovery.

**recover** - Sends an SNMP trap message when the switch recovers from a loopback condition.

**Default Setting**
None

**Command Mode**
Global Configuration

**Command Usage**
Refer to the `loopback-detection recover-time` command for information on conditions which constitute loopback recovery.

**Example**

```
Console(config)#loopback-detection trap both
Console(config)#
```

**loopback-detection release**
This command releases all interfaces currently shut down by the loopback detection feature.

**Syntax**

```
loopback-detection release
```

**Command Mode**
Privileged Exec

**Example**

```
Console#loopback-detection release
Console(config)#
```
**show loopback-detection**

This command shows loopback detection configuration settings for the switch or for a specified interface.

**Syntax**

```
show loopback-detection [interface]
```

**interface**

```
eternet unit/port
```

*unit* - Unit identifier. (Range: 1-8)

*port* - Port number. (Range: 1-28/52)

**Command Mode**

Privileged Exec

**Example**

```
Console#show loopback-detection
Loopback Detection Global Information
Global Status : Enabled
Transmit Interval : 10
Recover Time : 60
Action : Shutdown
Trap : None
Loopback Detection Port Information
Port Admin State Oper State
-------- ----------- ----------
Eth 1/ 1 Enabled Normal
Eth 1/ 2 Disabled Disabled
Eth 1/ 3 Disabled Disabled
:
Console#show loopback-detection ethernet 1/1
Loopback Detection Information of Eth 1/1
Admin State : Enabled
Oper State : Normal
Looped VLAN : None
Console#
```
Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 89: Address Table Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address-table aging-time</td>
<td>Sets the aging time of the address table</td>
<td>GC</td>
</tr>
<tr>
<td>mac-address-table static</td>
<td>Maps a static address to a port in a VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>clear mac-address-table dynamic</td>
<td>Removes any learned entries from the forwarding database</td>
<td>PE</td>
</tr>
<tr>
<td>show mac-address-table</td>
<td>Displays entries in the bridge-forwarding database</td>
<td>PE</td>
</tr>
<tr>
<td>show mac-address-table aging-time</td>
<td>Shows the aging time for the address table</td>
<td>PE</td>
</tr>
<tr>
<td>show mac-address-table count</td>
<td>Shows the number of MAC addresses used and the number of available MAC addresses</td>
<td>PE</td>
</tr>
</tbody>
</table>

**mac-address-table aging-time**

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

**Syntax**

```
mac-address-table aging-time seconds
no mac-address-table aging-time

seconds - Aging time. (Range: 10-844 seconds; 0 to disable aging)
```

**Default Setting**

300 seconds

**Command Mode**

Global Configuration

**Command Usage**

The aging time is used to age out dynamically learned forwarding information.

**Example**

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```
**mac-address-table static**  This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

**Syntax**

```
mac-address-table static mac-address interface interface vlan vlan-id [action]
no mac-address-table static mac-address vlan vlan-id
```

- `mac-address` - MAC address.
- `interface` - Interface identifier.
  - `ethernet unit/port`
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)
- `vlan-id` - VLAN ID (Range: 1-4094)
- `action`
  - `delete-on-reset` - Assignment lasts until the switch is reset.
  - `permanent` - Assignment is permanent.

**Default Setting**
No static addresses are defined. The default mode is **permanent**.

**Command Mode**
Global Configuration

**Command Usage**
The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

**Example**

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```
clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

**Syntax**

```
show mac-address-table [address mac-address [mask]] [interface interface] 
[interface vlan vlan-id] [sort [address | vlan | interface]]
```

- `mac-address` - MAC address.
- `mask` - Bits to match in the address.

**interface**

```
eternet unit/port
```

- `unit` - Unit identifier. (Range: 1)
- `port` - Port number. (Range: 1-28/52)

- `port-channel channel-id` (Range: 1-16)
- `vlan-id` - VLAN ID (Range: 1-4094)

- `sort` - Sort by address, vlan or interface.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Command Usage**

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learn - Dynamic address entries
  - Config - Static entry

- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means
to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”

◆ The maximum number of address entries is 16K.

Example

```
Console#show mac-address-table
Interface  MAC Address       VLAN Type     Life Time
--------- ----------------- ---- -------- -----------------
CPU      FC-0A-81-B7-C7-E0    1 CPU      Delete on Reset
Eth 1/1   00-E0-29-94-34-DE    1 Config   Delete on Reset
Eth 1/21  00-01-EC-F8-D8-D9    1 Learn    Delete on Timeout
```

```
show
mac-address-table
aging-time
This command shows the aging time for entries in the address table.

Default Setting
None

Command Mode
Privileged Exec

Example

```
Console#show mac-address-table aging-time
Aging Status : Enabled
Aging Time: 300 sec.
```

```
show
mac-address-table
count
This command shows the number of MAC addresses used and the number of available MAC addresses for the overall system or for an interface.

Syntax

```
show mac-address-table count interface interface
```

```
ethernet unit/port
```

```
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)
```

```
port-channel channel-id (Range: 1-16)
```

Default Setting
None

Command Mode
Privileged Exec
Example

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Eth 1/1
Total Address Count      :0
Static Address Count    :0
Dynamic Address Count   :0
Console#
```
Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 90: Spanning Tree Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree</td>
<td>Enables the spanning tree protocol</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree cisco-prestandard</td>
<td>Configures spanning tree operation to be compatible with Cisco prestandard versions</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree forward-time</td>
<td>Configures the spanning tree bridge forward time</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree hello-time</td>
<td>Configures the spanning tree bridge hello time</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree max-age</td>
<td>Configures the spanning tree bridge maximum age</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree mode</td>
<td>Configures STP, RSTP or MSTP mode</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree pathcost method</td>
<td>Configures the path cost method for RSTP/MSTP</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree priority</td>
<td>Configures the spanning tree bridge priority</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree mst configuration</td>
<td>Changes to MSTP configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree system-bpdus-flooding</td>
<td>Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled</td>
<td>GC</td>
</tr>
<tr>
<td>spanning-tree transmission-limit</td>
<td>Configures the transmission limit for RSTP/MSTP</td>
<td>GC</td>
</tr>
<tr>
<td>max-hops</td>
<td>Configures the maximum number of hops allowed in the region before a BPDU is discarded</td>
<td>MST</td>
</tr>
<tr>
<td>mst priority</td>
<td>Configures the priority of a spanning tree instance</td>
<td>MST</td>
</tr>
<tr>
<td>mst vlan</td>
<td>Adds VLANs to a spanning tree instance</td>
<td>MST</td>
</tr>
<tr>
<td>name</td>
<td>Configures the name for the multiple spanning tree</td>
<td>MST</td>
</tr>
<tr>
<td>revision</td>
<td>Configures the revision number for the multiple spanning tree</td>
<td>MST</td>
</tr>
<tr>
<td>spanning-tree bpdu-filter</td>
<td>Filters BPDUs for edge ports</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree bpdu-guard</td>
<td>Shuts down an edge port if it receives a BPDU</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree cost</td>
<td>Configures the spanning tree path cost of an interface</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree edge-port</td>
<td>Enables fast forwarding for edge ports</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree link-type</td>
<td>Configures the link type for RSTP/MSTP</td>
<td>IC</td>
</tr>
<tr>
<td>spanning-tree loopback-detection</td>
<td>Enables BPDU loopback detection for a port</td>
<td>IC</td>
</tr>
</tbody>
</table>
Spanning Tree Commands

This command enables the Spanning Tree Algorithm globally for the switch. Use the no form to disable it.

Syntax

```
[no] spanning-tree
```

Default Setting
Spanning tree is enabled.

Command Mode
Global Configuration

Command Usage
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant...
switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

**Example**

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

**spanning-tree cisco-prestandard**

This command configures spanning tree operation to be compatible with Cisco prestandard versions. Use the **no** form to restore the default setting.

```
[no] spanning-tree cisco-prestandard
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

Cisco prestandard versions prior to Cisco IOS Release 12.2(25)SEC do not fully follow the IEEE standard, causing some state machine procedures to function incorrectly. The command forces the spanning tree protocol to function in a manner compatible with Cisco prestandard versions.

**Example**

```
Console(config)#spanning-tree cisco-prestandard
Console(config)#
```

**spanning-tree forward-time**

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

**Syntax**

```
spanning-tree forward-time seconds
no spanning-tree forward-time
```

*seconds* - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or \(\left(\frac{\text{max-age}}{2}\right) + 1\).

**Default Setting**

15 seconds
Command Mode
Global Configuration

Command Usage
This command sets the maximum time (in seconds) a port will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

---

**spanning-tree hello-time**  
This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

**Syntax**

```
spanning-tree hello-time time

no spanning-tree hello-time
```

`time` - Time in seconds. (Range: 1-10 seconds).  
The maximum value is the lower of 10 or \([\text{max-age} / 2] - 1\).

**Default Setting**

2 seconds

Command Mode
Global Configuration

Command Usage
This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

Related Commands
- spanning-tree forward-time (467)
- spanning-tree max-age (469)
**spanning-tree max-age**  This command configures the spanning tree bridge maximum age globally for this switch. Use the `no` form to restore the default.

**Syntax**

```
spanning-tree max-age seconds

no spanning-tree max-age
```

- `seconds` - Time in seconds. (Range: 6-40 seconds)
  The minimum value is the higher of 6 or \(2 \times (\text{hello-time} + 1)\).
  The maximum value is the lower of 40 or \(2 \times (\text{forward-time} - 1)\).

**Default Setting**

20 seconds

**Command Mode**

Global Configuration

**Command Usage**

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

**Example**

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

**Related Commands**

- `spanning-tree forward-time (467)`
- `spanning-tree hello-time (468)`

**spanning-tree mode**  This command selects the spanning tree mode for this switch. Use the `no` form to restore the default.

**Syntax**

```
spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode
```

- `stp` - Spanning Tree Protocol (IEEE 802.1D)
- `rstp` - Rapid Spanning Tree Protocol (IEEE 802.1w)
- `mstp` - Multiple Spanning Tree (IEEE 802.1s)
Default Setting
rsstp

Command Mode
Global Configuration

Command Usage
◆ Spanning Tree Protocol
This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

◆ Rapid Spanning Tree Protocol
RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

■ STP Mode – If the switch receives an 802.1D BPDU after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

■ RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

◆ Multiple Spanning Tree Protocol

■ To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

■ A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

■ Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example
The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```
spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the no form to restore the default.

Syntax

```
spanning-tree pathcost method {long | short}
no spanning-tree pathcost method
```

- **long** - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.
- **short** - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Setting
Long method

Command Mode
Global Configuration

Command Usage
◆ The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 479) takes precedence over port priority (page 486).

◆ The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the no form to restore the default.

Syntax

```
spanning-tree priority priority
no spanning-tree priority
```

- **priority** - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting
32768
Command Mode
Global Configuration

Command Usage
Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example
```
Console(config)#spanning-tree priority 40960
Console(config)#
```

spanning-tree mst configuration
This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Setting
No VLANs are mapped to any MST instance. The region name is set the switch's MAC address.

Command Mode
Global Configuration

Example
```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

Related Commands
mst vlan (475)
mst priority (474)
name (476)
revision (476)
max-hops (474)

spanning-tree system-bpdu-flooding
This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the no form to restore the default.

Syntax
```
spanning-tree system-bpdu-flooding {to-all | to-vlan}
no spanning-tree system-bpdu-flooding
  to-all - Floods BPDUs to all other ports on the switch.
```
to-vlan - Floods BPDUs to all other ports within the receiving port’s native VLAN (i.e., as determined by port’s PVID).

Default Setting
Floods to all other ports in the same VLAN.

Command Mode
Global Configuration

Command Usage
The `spanning-tree system-bpdu-flooding` command has no effect if BPDU flooding is disabled on a port (see the `spanning-tree port-bpdu-flooding` command).

Example
```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

**spanning-tree transmission-limit**
This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the `no` form to restore the default.

Syntax
```
spanning-tree transmission-limit count
no spanning-tree transmission-limit
```

*count* - The transmission limit in seconds. (Range: 1-10)

Default Setting
3

Command Mode
Global Configuration

Command Usage
This command limits the maximum transmission rate for BPDUs.

Example
```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```
**max-hops**  This command configures the maximum number of hops in the region before a BPDU is discarded. Use the no form to restore the default.

**Syntax**

```
max-hops hop-number
```

*hop-number* - Maximum hop number for multiple spanning tree.

(Range: 1-40)

**Default Setting**

20

**Command Mode**

MST Configuration

**Command Usage**

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

**Example**

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

**mst priority**  This command configures the priority of a spanning tree instance. Use the no form to restore the default.

**Syntax**

```
mst instance-id priority priority
no mst instance-id priority
```

*instance-id* - Instance identifier of the spanning tree. (Range: 0-4094)

*priority* - Priority of the a spanning tree instance.

(Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

**Default Setting**

32768

**Command Mode**

MST Configuration
Command Usage
◆ MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

◆ You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

**mst vlan**  This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

```
[no] mst instance-id vlan vlan-range
```

- **instance-id** - Instance identifier of the spanning tree. (Range: 0-4094)
- **vlan-range** - Range of VLANs. (Range: 1-4094)

Default Setting
none

Command Mode
MST Configuration

Command Usage
◆ Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

◆ By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 16 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 476) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.
**Example**

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

**name**  
This command configures the name for the multiple spanning tree region in which this switch is located. Use the `no` form to clear the name.

**Syntax**
```
name name
```

- `name` - Name of the spanning tree.

**Default Setting**
Switch's MAC address

**Command Mode**
MST Configuration

**Command Usage**
The MST region name and revision number (page 476) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

**Example**

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

**Related Commands**
revision (476)

**revision**  
This command configures the revision number for this multiple spanning tree configuration of this switch. Use the `no` form to restore the default.

**Syntax**
```
revision number
```

- `number` - Revision number of the spanning tree. (Range: 0-65535)

**Default Setting**
0

**Command Mode**
MST Configuration
Command Usage
The MST region name (page 476) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example
```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands
name (476)

```
spanning-tree bpdu-filter
```
This command allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. Use the no form to disable this feature.

Syntax
```
[no] spanning-tree bpdu-filter
```

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ This command stops all Bridge Protocol Data Units (BPDUs) from being transmitted on configured edge ports to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.

◆ Before enabling BPDU Filter, the interface must first be configured as an edge port with the spanning-tree edge-port command.

Example
```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

Related Commands
spanning-tree edge-port (480)
**spanning-tree bpdu-guard**

This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form without any keywords to disable this feature, or with a keyword to restore the default settings.

**Syntax**

```
spanning-tree bpdu-guard [auto-recovery [interval interval]]
no spanning-tree bpdu-guard [auto-recovery [interval]]
```

- **auto-recovery** - Automatically re-enables an interface after the specified interval.
- **interval** - The time to wait before re-enabling an interface. (Range: 30-86400 seconds)

**Default Setting**

BPDU Guard: Disabled
Auto-Recovery: Disabled
Auto-Recovery Interval: 300 seconds

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- An edge port should only be connected to end nodes which do not generate BPDU. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If an interface is shut down by BPDU Guard, it must be manually re-enabled using the **no spanning-tree spanning-disabled** command if the auto-recovery interval is not specified.

- Before enabling BPDU Guard, the interface must be configured as an edge port with the **spanning-tree edge-port** command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

**Related Commands**

- **spanning-tree edge-port** (480)
- **spanning-tree spanning-disabled** (488)
spanning-tree cost  This command configures the spanning tree path cost for the specified interface. Use the no form to restore the default auto-configuration mode.

Syntax

spanning-tree cost  cost

no spanning-tree cost

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method, 1-200,000,000 for long path cost method) 9

Table 91: Recommended STA Path Cost Range

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Short Path Cost (IEEE 802.1D-1998)</th>
<th>Long Path Cost (IEEE 802.1D-2004)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>50-600</td>
<td>200,000-20,000,000</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>10-60</td>
<td>20,000-2,000,000</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>3-10</td>
<td>2,000-200,000</td>
</tr>
</tbody>
</table>

Default Setting
By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 92: Default STA Path Costs

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Short Path Cost (IEEE 802.1D-1998)</th>
<th>Long Path Cost (IEEE 802.1D-2004)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>65,535</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>65,535</td>
<td>100,000</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>10,000</td>
<td>10,000</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.

◆ Path cost takes precedence over port priority.

9. Use the spanning-tree pathcost method command to set the path cost method. The range displayed in the CLI prompt message shows the maximum value for path cost. However, note that the switch still enforces the rules for path cost based on the specified path cost method (long or short).
◆ When the path cost method (page 471) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

`spanning-tree edge-port` This command specifies an interface as an edge port. Use the `no` form to restore the default.

**Syntax**

```
spanning-tree edge-port [auto]
```

```
no spanning-tree edge-port
```

`auto` - Automatically determines if an interface is an edge port.

**Default Setting**

Auto

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```
spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the no form to restore the default.

Syntax

```
spanning-tree link-type {auto | point-to-point | shared}
```

```
no spanning-tree link-type
```

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

```
auto
```

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.

- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.

- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree loopback-detection

This command enables the detection and response to Spanning Tree loopback BPDU packets on the port. Use the no form to disable this feature.

Syntax

```
[no] spanning-tree loopback-detection
```

Default Setting

- Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)
Command Usage
◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).

◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

This command configures the response for loopback detection to block user traffic or shut down the interface. Use the no form to restore the default.

Syntax

```
spanning-tree loopback-detection action
```

```
no spanning-tree loopback-detection action
```

**block** - Blocks user traffic.

**shutdown** - Shuts down the interface.

**duration** - The duration to shut down the interface.

(Range: 60-86400 seconds)

Default Setting

block

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ If an interface is shut down by this command, and the release mode is set to “auto” with the spanning-tree loopback-detection release-mode command, the selected interface will be automatically enabled when the shutdown interval has expired.

◆ If an interface is shut down by this command, and the release mode is set to “manual,” the interface can be re-enabled using the spanning-tree loopback-detection release command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
```
spanning-tree loopback-detection release-mode

This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the no form to restore the default.

**Syntax**

```
spanning-tree loopback-detection release-mode {auto | manual}

no spanning-tree loopback-detection release-mode
```

**Default Setting**

auto

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

◆ If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
  - The port receives any other BPDU except for it's own, or;
  - The port's link status changes to link down and then link up again, or;
  - The port ceases to receive it's own BPDUs in a forward delay interval.

◆ If Port Loopback Detection is not enabled and a port receives it's own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).

◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

◆ When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the spanning-tree loopback-detection release command.

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```
spanning-tree loopback-detection trap

This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the no form to restore the default.

Syntax

[no] spanning-tree loopback-detection trap

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the no form to restore the default auto-configuration mode.

Syntax

spanning-tree mst instance-id cost

no spanning-tree mst instance-id cost

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 91 on page 479.

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in Table 92 on page 479.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

◆ Each spanning-tree instance is associated with a unique set of VLAN IDs.

10. Use the spanning-tree pathcost method command to set the path cost method.
◆ This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.

◆ Use the **no spanning-tree mst cost** command to specify auto-configuration mode.

◆ Path cost takes precedence over interface priority.

**Example**

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

**Related Commands**

**spanning-tree mst port-priority**

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

**Syntax**

```
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

- **instance-id** - Instance identifier of the spanning tree. (Range: 0-4094)
- **priority** - Priority for an interface. (Range: 0-240 in steps of 16)

**Default Setting**

128

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

◆ This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

◆ Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.
Example

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

`spanning-tree mst cost (484)`

**spanning-tree port-bpdu-flooding**

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the `no` form to restore the default setting.

**Syntax**

```
[no] spanning-tree port-bpdu-flooding
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port’s native VLAN as specified by the `spanning-tree system-bpdu-flooding` command.

- The `spanning-tree system-bpdu-flooding` command has no effect if BPDU flooding is disabled on a port by the `spanning-tree port-bpdu-flooding` command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

**spanning-tree port-priority**

This command configures the priority for the specified interface. Use the `no` form to restore the default.

**Syntax**

```
spanning-tree port-priority priority
no spanning-tree port-priority
```

`priority` - The priority for a port. (Range: 0-240, in steps of 16)
Default Setting
128

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

◆ Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

◆ The criteria used for determining the port role is based on root bridge ID, root path cost, designated bridge, designated port, port priority, and port number, in that order and as applicable to the role under question.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands
spanning-tree cost (479)

spanning-tree root-guard

This command prevents a designated port from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the no form to disable this feature.

Syntax
```
[no] spanning-tree root-guard
```

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.

◆ When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a
fixed recovery period. While in the discarding state, no traffic is forwarded across the port.

◆ Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.

◆ When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

Example

```console
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

**spanning-tree spanning-disabled** This command disables the spanning tree algorithm for the specified interface. Use the no form to re-enable the spanning tree algorithm for the specified interface.

**Syntax**

```
[no] spanning-tree spanning-disabled
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Example**

This example disables the spanning tree algorithm for port 5.

```console
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

**spanning-tree tc-prop-stop** This command stops the propagation of topology change notifications (TCN). Use the no form to allow propagation of TCN messages.

**Syntax**

```
[no] spanning-tree tc-prop-stop
```
Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
When this command is enabled on an interface, topology change information originating from the interface will still be propagated.

This command should not be used on an interface which is purposely configured in a ring topology.

Example
```
Console(config)#interface ethernet 1/1
Console(config-if)#spanning-tree tc-prop-stop
Console(config-if)#
```

spanning-tree loopback-detection release
This command manually releases a port placed in discarding state by loopback-detection.

Syntax
```
spanning-tree loopback-detection release interface

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)
```

Command Mode
Privileged Exec

Command Usage
Use this command to release an interface from discarding state if loopback detection release mode is set to “manual” by the spanning-tree loopback-detection release-mode command and BPDU loopback occurs.

Example
```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```
**spanning-tree protocol-migration**  This command re-checks the appropriate BPDU format to send on the selected interface.

**Syntax**

```
spanning-tree protocol-migration interface
  interface
    ethernet unit/port
      unit - Unit identifier. (Range: 1)
      port - Port number. (Range: 1-28/52)
    port-channel channel-id (Range: 1-16)
```

**Command Mode**
Privileged Exec

**Command Usage**
If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the `spanning-tree protocol-migration` command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

**Example**

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

**show spanning-tree**  This command shows the configuration for the common spanning tree (CST), for all instances within the multiple spanning tree (MST), or for a specific instance within the multiple spanning tree (MST).

**Syntax**

```
show spanning-tree [interface | mst instance-id | brief | stp-enabled-only]
  interface
    ethernet unit/port
      unit - Unit identifier. (Range: 1)
      port - Port number. (Range: 1-28/52)
    port-channel channel-id (Range: 1-16)
  instance-id - Instance identifier of the multiple spanning tree.
    (Range: 0-4094)
  brief - Shows a summary of global and interface settings.
```

---

- 490 -
**stp-enabled-only** - Displays global settings, and settings for interfaces for which STP is enabled.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Command Usage**
- Use the `show spanning-tree` command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.

- Use the `show spanning-tree interface` command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).

- Use the `show spanning-tree mst configuration` command to display the configuration name, revision level, and VLANs associated with each instance.

- Use the `show spanning-tree mst instance-id` command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST), including global settings and settings for all interfaces.

**Example**

```
Console#show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
Spanning Tree Mode : MSTP
Spanning Tree Enabled/Disabled : Enabled
Instance : 0
VLANs Configured : 1-4094
Priority : 32768
Bridge Hello Time (sec.) : 2
Bridge Max. Age (sec.) : 20
Bridge Forward Delay (sec.) : 15
Root Hello Time (sec.) : 2
Root Max. Age (sec.) : 20
Root Forward Delay (sec.) : 15
Max. Hops : 20
Remaining Hops : 20
Designated Root : 32768.0.0001ECF8D8C6
Current Root Port : 21
Current Root Cost : 100000
Number of Topology Changes : 5
Last Topology Change Time (sec.) : 11409
Transmission Limit : 3
Path Cost Method : Long
Flooding Behavior : To VLAN
Cisco Prestandard : Disabled

Eth 1/1 information
---------------------------------------------------------------
Admin Status : Enabled
Role : Disabled
State : Discarding
```
This example shows a brief summary of global and interface setting for the spanning tree.

```
Console#show spanning-tree brief
Spanning Tree Mode     : RSTP
Spanning Tree Enabled/Disabled : Enabled
Designated Root          : 32768.0000E8944000
Current Root Port (Eth)  : 1/24
Current Root Cost        : 10000

Interface Pri Designated  Designated Oper     STP    Role State Oper
Bridge ID       Port ID    Cost     Status            Edge
----------------- --------------------- ---------- -------- ------ ---- ----- ---
Eth 1/ 1  128 32768.0000E89382A0  128.1        100000 EN     DESG FWD   No
Eth 1/ 2  128 32768.0000E89382A0  128.2         10000 EN     DISB BLK   No
Eth 1/ 3  128 32768.0000E89382A0  128.3         10000 EN     DISB BLK   No
Eth 1/ 4  128 32768.0000E89382A0  128.4         10000 EN     DISB BLK   No
Eth 1/ 5  128 32768.0000E89382A0  128.5         10000 EN     DISB BLK   No
..
show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

**Command Mode**
Privileged Exec

**Example**

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-----------------------------------------------
Configuration Name : R&D
Revision Level     : 0

Instance VLANs
-----------------------------------------------
  0    1-4094
Console#
```
A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

### Table 93: VLAN Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GVRP and Bridge Extension</strong></td>
<td>Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB</td>
</tr>
<tr>
<td><strong>Editing VLAN Groups</strong></td>
<td>Sets up VLAN groups, including name, VID and state</td>
</tr>
<tr>
<td><strong>Configuring VLAN Interfaces</strong></td>
<td>Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP</td>
</tr>
<tr>
<td><strong>Displaying VLAN Information</strong></td>
<td>Displays VLAN groups, status, port members, and MAC addresses</td>
</tr>
<tr>
<td><strong>Configuring IEEE 802.1Q Tunneling</strong></td>
<td>Configures 802.1Q Tunneling (QinQ Tunneling)</td>
</tr>
<tr>
<td><strong>Configuring L2CP Tunneling</strong></td>
<td>Configures Layer 2 Control Protocol (L2CP) tunneling, either by discarding, processing, or transparently passing control packets across a QinQ tunnel</td>
</tr>
<tr>
<td><strong>Configuring Protocol-based VLANS</strong></td>
<td>Configures protocol-based VLANS based on frame type and protocol</td>
</tr>
<tr>
<td><strong>Configuring IP Subnet VLANS</strong></td>
<td>Configures IP Subnet-based VLANS</td>
</tr>
<tr>
<td><strong>Configuring MAC Based VLANS</strong></td>
<td>Configures MAC-based VLANS</td>
</tr>
<tr>
<td><strong>Configuring Voice VLANS</strong></td>
<td>Configures VoIP traffic detection and enables a Voice VLAN</td>
</tr>
</tbody>
</table>

* If a packet matches the rules defined by more than one of these functions, only one of them is applied, with the precedence being MAC-based, IP subnet-based, protocol-based, and then native port-based (see the switchport priority default command).
GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 94: GVRP and Bridge Extension Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge-ext gvrp</td>
<td>Enables GVRP globally for the switch</td>
<td>GC</td>
</tr>
<tr>
<td>garp timer</td>
<td>Sets the GARP timer for the selected function</td>
<td>IC</td>
</tr>
<tr>
<td>switchport forbidden vlan</td>
<td>Configures forbidden VLANs for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>switchport gvrp</td>
<td>Enables GVRP for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>show bridge-ext</td>
<td>Shows the global bridge extension configuration</td>
<td>PE</td>
</tr>
<tr>
<td>show garp timer</td>
<td>Shows the GARP timer for the selected function</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show gvrp configuration</td>
<td>Displays GVRP configuration for the selected interface</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

**bridge-ext gvrp**

This command enables GVRP globally for the switch. Use the **no** form to disable it.

**Syntax**

```
[no] bridge-ext gvrp
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

**Example**

```
Console(config)#bridge-ext gvrp
Console(config)#
```
**garp timer**  This command sets the values for the join, leave and leaveall timers. Use the no form to restore the timers' default values.

**Syntax**

```
garp timer {join | leave | leaveall} timer-value
no garp timer {join | leave | leaveall}
   {join | leave | leaveall} - Timer to set.
   timer-value - Value of timer.
   Ranges:
   join: 20-1000 centiseconds
   leave: 60-3000 centiseconds
   leaveall: 500-18000 centiseconds
```

**Default Setting**

join: 20 centiseconds  
leave: 60 centiseconds  
leaveall: 1000 centiseconds

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

◆ Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.

◆ Timer values are applied to GVRP for all the ports on all VLANs.

◆ Timer values must meet the following restrictions:

   ■ leave > (2 x join)
   ■ leaveall > leave

**Note:** Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```
**Related Commands**

`show garp timer (500)`

**switchport forbidden vlan**

This command configures forbidden VLANs. Use the `no` form to remove the list of forbidden VLANs.

**Syntax**

```
switchport forbidden vlan {add vlan-list | remove vlan-list}
no switchport forbidden vlan
```

- **add vlan-list** - List of VLAN identifiers to add.
- **remove vlan-list** - List of VLAN identifiers to remove.
- **vlan-list** - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

**Default Setting**

No VLANs are included in the forbidden list.

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.

- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

- GVRP cannot be enabled for ports set to Access mode (see the `switchport mode` command).

**Example**

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```
**switchport gvrp**  This command enables GVRP for a port. Use the **no** form to disable it.

**Syntax**

```
[no] switchport gvrp
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

GVRP cannot be enabled for ports set to Access mode using the **switchport mode** command.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

**show bridge-ext**  This command shows the configuration for bridge extension commands.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```
Console#show bridge-ext
Maximum Supported VLAN Numbers : 4094
Maximum Supported VLAN ID : 4094
Extended Multicast Filtering Services : No
Static Entry Individual Port : Yes
VLAN Version Number : 2
VLAN Learning : IVL
Configurable PVID Tagging : Yes
Local VLAN Capable : No
Traffic Classes : Enabled
Global GVRP Status : Disabled
GMRP : Disabled
Console#
```
**show garp timer**  This command shows the GARP timers for the selected interface.

**Syntax**

```
show garp timer [interface]
```

`interface`

```
eternet unit/port
```

- `unit` - Unit identifier. (Range: 1)
- `port` - Port number. (Range: 1-28/52)

```
port-channel channel-id (Range: 1-16)
```

**Default Setting**

Shows all GARP timers.

**Command Mode**

Normal Exec, Privileged Exec

---

**Table 95: show bridge-ext - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Supported VLAN Numbers</td>
<td>The maximum number of VLANs supported on this switch.</td>
</tr>
<tr>
<td>Maximum Supported VLAN ID</td>
<td>The maximum configurable VLAN identifier supported on this switch.</td>
</tr>
<tr>
<td>Extended Multicast Filtering Services</td>
<td>This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).</td>
</tr>
<tr>
<td>Static Entry Individual Port</td>
<td>This switch allows static filtering for unicast and multicast addresses. (Refer to the <code>mac-address-table static</code> command.)</td>
</tr>
<tr>
<td>VLAN Learning</td>
<td>This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.</td>
</tr>
<tr>
<td>Configurable PVID Tagging</td>
<td>This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to the <code>switchport allowed vlan</code> command.)</td>
</tr>
<tr>
<td>Local VLAN Capable</td>
<td>This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.</td>
</tr>
<tr>
<td>Traffic Classes</td>
<td>This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Commands” on page 541.)</td>
</tr>
<tr>
<td>Global GVRP Status</td>
<td>GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This field shows if GVRP is globally enabled or disabled. (Refer to the <code>bridge-ext gvrp</code> command.)</td>
</tr>
</tbody>
</table>
Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
    Join Timer:     20 centiseconds
    Leave Timer:    60 centiseconds
    Leaveall Timer: 1000 centiseconds
Console#
```

Related Commands
garp timer (497)

**show gvrp configuration**
This command shows if GVRP is enabled.

Syntax

```
show gvrp configuration [interface]

interface

    ethernet unit/port

    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)
```

Default Setting
Shows both global and interface-specific configuration.

Command Mode
Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
    GVRP Configuration : Disabled
Console#
```

Editing VLAN Groups

Table 96: Commands for Editing VLAN Groups

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan database</td>
<td>Enters VLAN database mode to add, change, and delete VLANs</td>
<td>GC</td>
</tr>
<tr>
<td>vlan</td>
<td>Configures a VLAN, including VID, name and state</td>
<td>VC</td>
</tr>
</tbody>
</table>
**vlan database**  This command enters VLAN database mode. All commands in this mode will take effect immediately.

**Default Setting**
None

**Command Mode**
Global Configuration

**Command Usage**
◆ Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the show vlan command.

◆ Use the interface **vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the show running-config command.

**Example**

```
Console(config)#vlan database
Console(config-vlan)#
```

**Related Commands**
show vlan (513)

**vlan**  This command configures a VLAN. Use the no form to restore the default settings or delete a VLAN.

**Syntax**

```
vlan  vlan-id  [name  vlan-name]  media  ethernet  [state  {active  |  suspend}]  [rspan]
no  vlan  vlan-id  [name  |  state]
```

- **vlan-id** - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094)
- **name** - Keyword to be followed by the VLAN name.
- **vlan-name** - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
**state** - Keyword to be followed by the VLAN state.

*active* - VLAN is operational.

*suspend* - VLAN is suspended. Suspended VLANs do not pass packets.

**rspan** - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPAN cannot include VLAN 1 (the switch's default VLAN). Nor should it include VLAN 4093 (which is used for switch clustering). Configuring VLAN 4093 for other purposes may cause problems in the Clustering operation. For more information on configuring RSPAN through the CLI, see “RSPAN Mirroring Commands” on page 428.

**Default Setting**
By default only VLAN 1 exists and is active.

**Command Mode**
VLAN Database Configuration

**Command Usage**
◆ **no vlan vlan-id** deletes the VLAN.
◆ **no vlan vlan-id name** removes the VLAN name.
◆ **no vlan vlan-id state** returns the VLAN to the default state (i.e., active).
◆ You can configure up to 4094 VLANs on the switch.

**Example**
The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

**Related Commands**
show vlan (513)

---

**Configuring VLAN Interfaces**

**Table 97: Commands for Configuring VLAN Interfaces**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface vlan</td>
<td>Enters interface configuration mode for a specified VLAN</td>
<td>IC</td>
</tr>
<tr>
<td>switchport acceptable-</td>
<td>Configures frame types to be accepted by an interface</td>
<td>IC</td>
</tr>
<tr>
<td>frame-types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>switchport allowed vlan</td>
<td>Configures the VLANs associated with an interface</td>
<td>IC</td>
</tr>
</tbody>
</table>
interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface. Use the no form to change a Layer 3 normal VLAN back to a Layer 2 interface.

Syntax

    [no] interface vlan vlan-id

    vlan-id - ID of the configured VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Command Usage

◆ Creating a “normal” VLAN with the vlan command initializes it as a Layer 2 interface. To change it to a Layer 3 interface, use the interface command to enter interface configuration for the desired VLAN, enter any Layer 3 configuration commands, and save the configuration settings.

◆ To change a Layer 3 normal VLAN back to a Layer 2 VLAN, use the no interface command.
Example
The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands
shutdown (383)
interface (378)
vlan (502)

**switchport acceptable-frame-types**
This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

**Syntax**

```
switchport acceptable-frame-types {all | tagged}
no switchport acceptable-frame-types
```

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

**Default Setting**
All frame types

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

**Example**
The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

**Related Commands**
switchport mode (508)
**switchport allowed vlan**  This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

**Syntax**

```
switchport allowed vlan {vlan-list | add vlan-list [tagged | untagged] | remove vlan-list}
```

```
no switchport allowed vlan
```

- `vlan-list` - If a VLAN list is entered without using the **add** option, the interface is assigned to the specified VLANs, and membership in all previous VLANs is removed. The interface is added as a tagged member if `switchport mode` is set to hybrid or access, or as an untagged member if switchport mode is set to trunk.

Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

- **add vlan-list** - List of VLAN identifiers to add. When the **add** option is used, the interface is assigned to the specified VLANs, and membership in all previous VLANs is retained.

- **remove vlan-list** - List of VLAN identifiers to remove.

**Default Setting**

All ports are assigned to VLAN 1 by default.

The default frame type is untagged.

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- If a port or trunk has switchport mode set to **access**, then only one VLAN can be added with this command. If a VLAN list is specified, only the last VLAN in the list will be added to the interface.

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.

- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.

- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.

- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
◆ If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example
The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

```
switchport ingress-filtering
```
This command enables ingress filtering for an interface. Use the no form to restore the default.

Syntax

```
[no] switchport ingress-filtering
```

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

◆ Ingress filtering only affects tagged frames.

◆ If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).

◆ If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

◆ Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example
The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```
**switchport mode**  This command configures the VLAN membership mode for a port. Use the `no` form to restore the default.

**Syntax**

```
switchport mode (access | hybrid | trunk)
```

no switchport mode

- **access** - Specifies an access VLAN interface. The port transmits and receives untagged frames on a single VLAN only.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port’s default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

**Default Setting**
Hybrid mode, with the PVID set to VLAN 1.

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
Access mode is mutually exclusive with VLAN trunking (see the `vlan-trunking` command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

**Example**
The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

**Related Commands**
- `switchport acceptable-frame-types (505)`
**switchport native vlan**  This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

**Syntax**

```
switchport native vlan vlan-id
no switchport native vlan
```

- **vlan-id** - Default VLAN ID for a port. (Range: 1-4094)

**Default Setting**

VLAN 1

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.

- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

**Example**

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

**switchport trunk allowed vlan**  This command restricts the VLANs associated with a trunk (operating in hybrid or 802.1Q trunk mode), adding the interface as a tagged member. Use the **no** form to restore the default setting.

**Syntax**

```
switchport trunk allowed vlan {(add | remove) vlan-list}
no switchport trunk allowed vlan
```

- **add vlan-list** - List of VLAN identifiers to add.
- **remove vlan-list** - List of VLAN identifiers to remove.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport trunk allowed vlan add 3
```

- **vlan-list** - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).
Chapter 18 | VLAN Commands
Configuring VLAN Interfaces

Default Setting
None

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ VLAN trunking allows unknown VLAN groups to pass through the specified interface. Use the `switchport trunk allowed vlan` command to restrict the VLANs associated with a trunk (operating in hybrid or 802.1Q trunk mode), adding the interface as a tagged member

◆ The native VLAN cannot be specified as a trunk member by this command.

Example
The following example restricts trunk members to VLANs 2 and 3 on port 10:

```
Console(config)#interface ethernet 1/10
Console(config-if)#switchport trunk allowed vlan add 2,3
Console(config-if)#
```

**switchport trunk native vlan**
This command configures the PVID (native VLAN) of an interface that is operating in 802.1Q trunk mode, and also sets it to be an untagged member of the native VLAN. Use the `no` form to restore to the previous PVID and change the membership of the VLAN associated with the previous PVID back to tagged mode.

**Syntax**

```
switchport trunk native vlan vlan-id
no switchport trunk native vlan
```

`vlan-id` - Default VLAN ID for a port. (Range: 1-4094)

**Default Setting**
VLAN 1

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The `switchport allowed vlan` command will display an error message if you attempt to configure an 802.1Q trunk to be untagged member of a VLAN, even if the specified VLAN is the trunk’s native VLAN. The `switchport trunk native vlan` command is therefore more useful for configuring the members of an 802.1Q trunk.
Example
The following example shows how to set the PVID for port 15 (which is operating as an 802.1 trunk) to VLAN 2:

```console
Console(config)#interface ethernet 1/15
Console(config-if)#switchport allowed vlan add 2
Console(config-if)#switchport mode trunk
Console(config-if)#switchport trunk native vlan 2
Console(config-if)#end
Console#show interfaces switchport ethernet 1/16
Information of Eth 1/16
Broadcast Threshold : Enabled, 64 Kbits/second
Multicast Threshold : Disabled
Unknown Unicast Threshold : Disabled
LACP Status : Disabled
Ingress Rate Limit : Disabled, 64 Kbits per second
Egress Rate Limit : Disabled, 1000000 Kbits per second
VLAN Membership Mode : Trunk
Ingress Rule : Disabled
Acceptable Frame Type : All frames
Native VLAN : 2
Priority for Untagged Traffic : 0
GVRP Status : Disabled
Allowed VLAN : 1(t), 2(u)
Forbidden VLAN :
802.1Q-Tunnel Status : Disabled
802.1Q-Tunnel Mode : Normal
802.1Q-Tunnel TPID : 8100 (Hex)
Console#
```

**vlan-trunking** This command allows unknown VLAN groups to pass through the specified interface. Use the no form to disable this feature.

**Syntax**

```
[no] vlan-trunking
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- Use this command to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.
Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- VLAN trunking is mutually exclusive with the “access” switchport mode (see the switchport mode command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).

- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

**Example**
The following example enables VLAN trunking on ports 27 and 28 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/27
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/28
Console(config-if)#vlan-trunking
Console(config-if)#
```
Displaying VLAN Information

This section describes commands used to display VLAN information.

Table 98: Commands for Displaying VLAN Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces status vlan</td>
<td>Displays status for the specified VLAN interface</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays the administrative and operational status of an interface</td>
<td>NE, PE</td>
</tr>
<tr>
<td>show vlan</td>
<td>Shows VLAN information</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

**show vlan** This command shows VLAN information.

**Syntax**

```
show vlan [id vlan-id | name vlan-name]
```

- **id** - Keyword to be followed by the VLAN ID.
- **vlan-id** - ID of the configured VLAN. (Range: 1-4094)
- **name** - Keyword to be followed by the VLAN name.
- **vlan-name** - ASCII string from 1 to 32 characters.

**Default Setting**

Shows all VLANs.

**Command Mode**

Normal Exec, Privileged Exec

**Example**

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID: 1
Type: Static
Name: DefaultVlan
Status: Active
Ports/Port Channels: Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S) Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S) Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S) Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S) Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S) Eth1/26(S) Eth1/27(S) Eth1/28(S)

Console#
```
IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider’s network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer’s original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 99: 802.1Q Tunneling Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1q-tunnel system-tunnel-control</td>
<td>Configures the switch to operate in normal mode or QinQ mode</td>
<td>GC</td>
</tr>
<tr>
<td>dot1q-tunnel tpid</td>
<td>Sets the Tag Protocol Identifier (TPID) value of a tunnel port</td>
<td>GC</td>
</tr>
<tr>
<td>switchport dot1q-tunnel mode</td>
<td>Configures an interface as a QinQ tunnel port</td>
<td>IC</td>
</tr>
<tr>
<td>switchport dot1q-tunnel service match cvid</td>
<td>Creates a CVLAN to SPVLAN mapping entry</td>
<td>IC</td>
</tr>
<tr>
<td>show dot1q-tunnel</td>
<td>Displays the configuration of QinQ tunnel ports</td>
<td>PE</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays port QinQ operational status</td>
<td>PE</td>
</tr>
</tbody>
</table>

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (dot1q-tunnel system-tunnel-control).

2. Create a SPVLAN (vlan).

3. Configure the QinQ tunnel access port to dot1Q-tunnel access mode (switchport dot1q-tunnel mode).

4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See dot1q-tunnel tpid.)

5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (switchport allowed vlan).

6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (switchport native vlan).

7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode (switchport dot1q-tunnel mode).
8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member
(switchport allowed vlan).

Limitations for QinQ

◆ The native VLAN for the tunnel uplink ports and tunnel access ports cannot be
the same. However, the same service VLANs can be set on both tunnel port
types.

◆ IGMP Snooping should not be enabled on a tunnel access port.

◆ If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel
uplink port may be disabled if the spanning tree structure is automatically
reconfigured to overcome a break in the tree. It is therefore advisable to disable
spanning tree on these ports.

dot1q-tunnel system-tunnel-control

This command sets the switch to operate in QinQ mode. Use the no form to disable
QinQ operating mode.

Syntax

[no] dot1q-tunnel system-tunnel-control

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be
functional.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

Related Commands

show dot1q-tunnel (520)
show interfaces switchport (389)
**dot1q-tunnel tpid**  This command sets the Tag Protocol Identifier (TPID) value for all ports. Use the `no` form to restore the default setting.

**Syntax**

```
dot1q-tunnel tpid tpid
no dot1q-tunnel tpid
```

*tpid* – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

**Default Setting**

0x8100

**Command Mode**

Global Configuration

**Command Usage**

- Use the **dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on all ports. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- The specified ethertype is set for all ports, including Uplink and Access tunnel ports (using the switchport dot1q-tunnel mode command), as well as normal ports that are not participating in any tunnel. However, the specified ethertype is only processed for ports configured in Uplink mode. If the port is in Access tunnel mode, received packets are processed as untagged packets.

- Avoid using well-known ethertypes for the TPID unless you can eliminate all side effects. For example, setting the TPID to 0800 hexadecimal (which is used for IPv4) will interfere with management access through the web interface.

**Example**

```
Console(config)#dot1q-tunnel tpid 9100
Console(config)#
```

**Related Commands**

* show interfaces switchport (389)
**switchport dot1q-tunnel mode** This command configures an interface as a QinQ tunnel port. Use the no form to disable QinQ on the interface.

**Syntax**

```
switchport dot1q-tunnel mode {access | uplink}
no switchport dot1q-tunnel mode
```

- **access** – Sets the port as an 802.1Q tunnel access port.
- **uplink** – Sets the port as an 802.1Q tunnel uplink port.

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- QinQ tunneling must be enabled on the switch using the **dot1q-tunnel system-tunnel-control** command before the **switchport dot1q-tunnel mode** interface command can take effect.

- When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider's tag added to the outer tag.

- When a tunnel uplink port receives a packet from the service provider, the outer service provider's tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

**Related Commands**

- `show dot1q-tunnel (520)`
- `show interfaces switchport (389)`
switchport dot1q-tunnel service match cvid

This command creates a CVLAN to SPVLAN mapping entry. Use the **no** form to delete a VLAN mapping entry.

**Syntax**

```
switchport dot1q-tunnel service svid match cvid cvid
```

- `svid` - VLAN ID for the outer VLAN tag (Service Provider VID). (Range: 1-4094)
- `cvid` - VLAN ID for the inner VLAN tag (Customer VID). (Range: 1-4094)

**Default Setting**

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- The inner VLAN tag of a customer packet entering the edge router of a service provider’s network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. This process is performed in a transparent manner.

- When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.

- Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider’s network for traffic arriving from specified inbound customer VLANs.

- Note that all customer interfaces should be configured as access interfaces (that is, a user-to-network interface) and service provider interfaces as uplink interfaces (that is, a network-to-network interface). Use the `switchport dot1q-tunnel mode uplink` command to set an interface to access or uplink mode.

**Example**

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet’s CVID is 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2
Console(config-if)#
```
The following example maps C-VLAN 10 to S-VLAN 100, C-VLAN 20 to S-VLAN 200 and C-VLAN 30 to S-VLAN 300 for ingress traffic on port 1 of Switches A and B.

Figure 4: Mapping QinQ Service VLAN to Customer VLAN

Step 1. Configure Switch A and B.

1. Create VLANs 100, 200 and 300.
   
   Console(config)#vlan database
   Console(config-vlan)#vlan 100,200,300 media ethernet state active

2. Enable QinQ.
   
   Console(config)#dot1q-tunnel system-tunnel-control

3. Configure port 2 as a tagged member of VLANs 100, 200 and 300 using uplink mode.
   
   Console(config)#interface ethernet 1/2
   Console(config-if)#switchport allowed vlan add 100,200,300 tagged
   Console(config-if)#switchport dot1q-tunnel mode uplink

4. Configure port 1 as an untagged member of VLANs 100, 200 and 300 using access mode.
   
   Console(config)#interface ethernet 1/1
   Console(config-if)#switchport allowed vlan add 100,200,300 untagged
   Console(config-if)#switchport dot1q-tunnel mode access

5. Configure the following selective QinQ mapping entries.
   
   Console(config)#interface ethernet 1/1
   Console(config-if)#switchport dot1q-tunnel service 100 match cvid 10
   Console(config-if)#switchport dot1q-tunnel service 200 match cvid 20
   Console(config-if)#switchport dot1q-tunnel service 300 match cvid 30

6. Configure port 1 as member of VLANs 10, 20 and 30 to avoid filtering out incoming frames tagged with VID 10, 20 or 30 on port 1.
   
   Console(config)#interface ethernet 1/1
   Console(config-if)#switchport allowed vlan add 10,20,30

7. Verify configuration settings.

   Console#show dot1q-tunnel service
   802.1Q Tunnel Service Subscriptions

<table>
<thead>
<tr>
<th>Port</th>
<th>Match C-VID</th>
<th>S-VID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>Eth 1/1</td>
<td>20</td>
<td>200</td>
</tr>
<tr>
<td>Eth 1/1</td>
<td>30</td>
<td>300</td>
</tr>
</tbody>
</table>
Step 2. Configure Switch C.

1. Create VLAN 100, 200 and 300.
   
   ```
   Console(config)#vlan database
   Console(config-vlan)#vlan 100,200,300 media ethernet state active
   ```

2. Configure port 1 and port 2 as tagged members of VLAN 100, 200 and 300.
   
   ```
   Console(config)#interface ethernet 1/1,2
   Console(config-if)#switchport allowed vlan add 100,200,300 tagged
   ```

**show dot1q-tunnel** This command displays information about QinQ tunnel ports.

**Syntax**

```
show dot1q-tunnel [interface interface [service svid] | service [svid]]
```

- **interface**
  - `ethernet unit/port`
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)

- **port-channel** `channel-id` (Range: 1-16)
  - `svid` - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094)

**Command Mode**

Privileged Exec

**Example**

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel
802.1Q Tunnel Status : Enabled
TPID is 0x8100

Port     Mode
-------- -----
Eth 1/ 1 Access
Eth 1/ 2 Uplink
Eth 1/ 3 Normal
Eth 1/ 4 Normal
Eth 1/ 3 Normal

Console#show dot1q-tunnel interface ethernet 1/5
802.1Q Tunnel Service Subscriptions

Port     Match C-VID S-VID
--------- ---------------
Eth 1/ 5    1   100
```
Console#show dot1q-tunnel service 100
802.1Q Tunnel Service Subscriptions

<table>
<thead>
<tr>
<th>Port</th>
<th>Match C-VID</th>
<th>S-VID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/5</td>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>Eth 1/6</td>
<td>1</td>
<td>100</td>
</tr>
</tbody>
</table>

Console#

Related Commands

switchport dot1q-tunnel mode (517)

Configuring L2CP Tunneling

This section describes the commands used to configure Layer 2 Protocol Tunneling (L2PT).

Table 100: L2 Protocol Tunnel Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel tunnel-dmac</td>
<td>Configures the destination address for Layer 2 Protocol Tunneling</td>
<td>GC</td>
</tr>
<tr>
<td>switchport l2protocol-tunnel</td>
<td>Enables Layer 2 Protocol Tunneling for the specified protocol</td>
<td>IC</td>
</tr>
<tr>
<td>show l2protocol-tunnel</td>
<td>Shows settings for Layer 2 Protocol Tunneling</td>
<td>PE</td>
</tr>
</tbody>
</table>

l2protocol-tunnel tunnel-dmac

This command configures the destination address for Layer 2 Protocol Tunneling (L2PT). Use the no form to restore the default setting.

Syntax

l2protocol-tunnel tunnel-dmac mac-address

mac-address – The switch rewrites the destination MAC address in all upstream L2PT protocol packets (i.e, STP BPDUs) to this value, and forwards them on to uplink ports. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

Default Setting
01-12-CF-.00-00-02, proprietary tunnel address

Command Mode
Global Configuration

Command Usage

◆ When L2PT is not used, protocol packets (such as STP) are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer’s network.
L2PT can be used to pass various types of protocol packets belonging to the same customer transparently across a service provider's network. In this way, normally segregated network segments can be configured to function inside a common protocol domain.

L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address (for example, the spanning tree protocol uses 10-12-CF-00-00-02), a reserved address for other specified protocol types (as defined in IEEE 802.1ad – Provider Bridges), or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site (via all of the appropriate tunnel ports and access ports connected to the same metro VLAN).

The way in which L2PT processes packets is based on the following criteria – (1) packet is received on a QinQ uplink port, (2) packet is received on a QinQ access port, or (3) received packet is Cisco-compatible L2PT (i.e., as indicated by a proprietary MAC address).

Processing protocol packets defined in IEEE 802.1ad – Provider Bridges

When an IEEE 802.1ad protocol packet is received on an uplink port (i.e., an 802.1Q tunnel ingress port connecting the edge switch to the service provider network)

- with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN tag), it is forwarded to all QinQ uplink ports and QinQ access ports in the same S-VLAN for which L2PT is enabled for that protocol.
- with the destination address 01-80-C2-00-00-01~0A (S-VLAN tag), it is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

When a protocol packet is received on an access port (i.e., an 802.1Q trunk port connecting the edge switch to the local customer network)

- with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN), and
  - L2PT is enabled on the port, the frame is forwarded to all QinQ uplink ports and QinQ access ports on which L2PT is enabled for that protocol in the same S-VLAN.
  - L2PT is disabled on the port, the frame is decapsulated and processed locally by the switch if the protocol is supported.

---

11. Access ports in this context are 802.1Q trunk ports.
with destination address 01-80-C2-00-00-01~0A (S-VLAN), the frame is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

**Processing Cisco-compatible protocol packets**

- When a Cisco-compatible L2PT packet is received on an uplink port, and
  - recognized as a CDP/VTP/STP/PVST+ protocol packet (where STP means STP/RSTP/MSTP), it is forwarded to the following ports in the same S-VLAN: (a) all access ports for which L2PT has been disabled, and (b) all uplink ports.
  - recognized as a Generic Bridge PDU Tunneling (GBPT) protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), it is forwarded to the following ports in the same S-VLAN:
    - other access ports for which L2PT is enabled after decapsulating the packet and restoring the proper protocol and MAC address information.
    - all uplink ports.
- When a Cisco-compatible L2PT packet is received on an access port, and
  - recognized as a CDP/VTP/STP/PVST+ protocol packet, and
    - L2PT is enabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is enabled, and (b) uplink ports after rewriting the destination address to make it a GBPT protocol packet (i.e., setting the destination address to 01-00-0C-CD-CD-D0).
    - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
  - recognized as a GBPT protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), and
    - L2PT is enabled on this port, it is forwarded to other access ports in the same S-VLAN for which L2PT is enabled
    - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
- For L2PT to function properly, QinQ must be enabled on the switch using the `dot1q-tunnel system-tunnel-control` command, and the interface configured to 802.1Q tunnel mode using the `switchport dot1q-tunnel mode` command.
Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#l2protocol-tunnel tunnel-dmac 01-80-C2-00-00-01
Console(config-)#
```

**switchport l2protocol-tunnel**

This command enables Layer 2 Protocol Tunneling (L2PT) for the specified protocol. Use the **no** form to disable L2PT for the specified protocol.

**Syntax**

```
switchport l2protocol-tunnel {cdp | lldp | pvst+ | spanning-tree | vtp}
```

- **cdp** - Cisco Discovery Protocol
- **lldp** - Link Layer Discovery Protocol
- **pvst+** - Cisco Per VLAN Spanning Tree Plus
- **spanning-tree** - Spanning Tree (STP, RSTP, MSTP)
- **vtp** - Cisco VLAN Trunking Protocol

**Default Setting**

Disabled for all protocols

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- Refer to the Command Usage section for the **l2protocol-tunnel tunnel-dmac** command.

- For L2PT to function properly, QinQ must be enabled on the switch using the **dot1q-tunnel system-tunnel-control** command, and the interface configured to 802.1Q tunnel mode using the **switchport dot1q-tunnel mode** command.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#switchport l2protocol-tunnel spanning-tree
Console(config-if)#
```
show l2protocol-tunnel

This command shows settings for Layer 2 Protocol Tunneling (L2PT).

**Command Mode**
Privileged Exec

**Example**

```
Console#show l2protocol-tunnel
Layer 2 Protocol Tunnel
Tunnel MAC Address : 01-12-CF-00-00-00
Interface    Protocol
-----------------------------------------------
Eth 1/1      Spanning Tree
Console#
```

---

### Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

#### Table 101: Protocol-based VLAN Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol-vlan</td>
<td>Create a protocol group, specifying the supported protocols</td>
<td>GC</td>
</tr>
<tr>
<td>protocol-group</td>
<td>Maps a protocol group to a VLAN</td>
<td>IC</td>
</tr>
<tr>
<td>show protocol-vlan</td>
<td>Shows the configuration of protocol groups</td>
<td>PE</td>
</tr>
<tr>
<td>protocol-vlan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>protocol-group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show interfaces protocol-vlan</td>
<td>Shows the interfaces mapped to a protocol group and the corresponding VLAN</td>
<td>PE</td>
</tr>
</tbody>
</table>

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 502). Although not mandatory, we suggest configuring a separate VLAN for each
major protocol running on your network. Do not add port members at this time.

2. Create a protocol group for each of the protocols you want to assign to a VLAN using the `protocol-vlan protocol-group` command (Global Configuration mode).

3. Then map the protocol for each interface to the appropriate VLAN using the `protocol-vlan protocol-group` command (Interface Configuration mode).

4. Configure the VLAN groups for each interface using the `switchport allowed vlan` command.

**protocol-vlan protocol-group**

(Concatrating Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the `no` form to remove a protocol group.

**Syntax**

```
protocol-vlan protocol-group group-id [add | remove] frame-type frame
protocol-type protocol
```

### Default Setting

No protocol groups are configured.

### Command Mode

Global Configuration

### Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type arp
```

12. SNAP frame types are not supported by this switch due to hardware limitations.
This command maps a protocol group to a VLAN for the current interface. Use the no form to remove the protocol mapping for this interface.

**Syntax**

```
protocol-vlan protocol-group group-id vlan vlan-id priority priority
no protocol-vlan protocol-group group-id vlan
```

- `group-id` - Group identifier of this protocol group. (Range: 1-2147483647)
- `vlan-id` - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)
- `priority` - The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

**Default Setting**
No protocol groups are mapped for any interface.
Priority: 0

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the vlan command), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.
Example
The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

**show protocol-vlan protocol-group**
This command shows the frame and protocol type associated with protocol groups.

**Syntax**
```
show protocol-vlan protocol-group [group-id]
```

*group-id* - Group identifier for a protocol group. (Range: 1-2147483647)

**Default Setting**
All protocol groups are displayed.

**Command Mode**
Privileged Exec

**Example**
This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group
Protocol Group ID   Frame Type    Protocol Type
------------------ ------------- ---------------
1                  ethernet     08 00
Console#
```

**show interfaces protocol-vlan protocol-group**
This command shows the mapping from protocol groups to VLANs for the selected interfaces.

**Syntax**
```
show interfaces protocol-vlan protocol-group [interface]
interface
   ethernet unit/port
      unit - Unit identifier. (Range: 1)
      port - Port number. (Range: 1-28/52)
   port-channel channel-id (Range: 1-16)
```
Default Setting
The mapping for all interfaces is displayed.

Command Mode
Privileged Exec

Example
This shows that traffic entering Port 1 that matches the specifications for protocol
group 1 will be mapped to VLAN 2:

```console
Console# show interfaces protocol-vlan protocol-group
        Port     ProtocolGroup ID    VLAN ID
    ---------- ------------------  -----------
        Eth 1/1                  1       vlan2
Console#
```

Configuring IP Subnet VLANs
When using IEEE 802.1Q port-based VLAN classification, all untagged frames
received by a port are classified as belonging to the VLAN whose VID (PVID) is
associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of
untagged ingress frames are checked against the IP subnet-to-VLAN mapping
table. If an entry is found for that subnet, these frames are assigned to the VLAN
indicated in the entry. If no IP subnet is matched, the untagged frames are classified
as belonging to the receiving port's VLAN ID (PVID).

Table 102: IP Subnet VLAN Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet-vlan</td>
<td>Defines the IP Subnet VLANs</td>
<td>GC</td>
</tr>
<tr>
<td>show subnet-vlan</td>
<td>Displays IP Subnet VLAN settings</td>
<td>PE</td>
</tr>
</tbody>
</table>
This command configures IP Subnet VLAN assignments. Use the `no` form to remove an IP subnet-to-VLAN assignment.

**Syntax**

```
subnet-vlan subnet ip-address mask vlan vlan-id [priority priority]
```

```
no subnet-vlan subnet {ip-address mask | all}
```

- `ip-address` – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- `mask` – This mask identifies the host address bits of the IP subnet.
- `vlan-id` – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4094)
- `priority` – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

**Default Setting**

Priority: 0

**Command Mode**

Global Configuration

**Command Usage**

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask. The specified VLAN need not be an existing VLAN.

- After creating an IP-subnet VLAN, be sure to configure the VLAN for selected interfaces using the `switchport allowed vlan` command.

- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.

- The IP subnet cannot be a broadcast or multicast IP address.

- When MAC-based, IP subnet-based, or protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

**Example**

The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```
show subnet-vlan  This command displays IP Subnet VLAN assignments.

**Command Mode**
Privileged Exec

**Command Usage**
- Use this command to display subnet-to-VLAN mappings.
- The last matched entry is used if more than one entry can be matched.

**Example**
The following example displays all configured IP subnet-based VLANs.

```
Console#show subnet-vlan
IP Address       Mask             VLAN ID  Priority
---------------  ---------------  -------  --------
192.168.12.0     255.255.255.128        1         0
192.168.12.128   255.255.255.192        3         0
192.168.12.192   255.255.255.224        4         0
192.168.12.224   255.255.255.240        5         0
192.168.12.240   255.255.255.248        6         0
192.168.12.248   255.255.255.252        7         0
192.168.12.252   255.255.255.254        8         0
192.168.12.254   255.255.255.255        9         0
192.168.12.255   255.255.255.255       10         0
Console#
```

### Configuring MAC Based VLANs

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port’s VLAN ID (PVID).

**Table 103: MAC Based VLAN Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-vlan</td>
<td>Defines the IP Subnet VLANs</td>
<td>GC</td>
</tr>
<tr>
<td>show mac-vlan</td>
<td>Displays IP Subnet VLAN settings</td>
<td>PE</td>
</tr>
</tbody>
</table>
This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

**Syntax**

```
mac-vlan mac-address mac-address [mask mask-address] vlan vlan-id [priority priority]
```

```
no mac-vlan mac-address [mac-address [mask mask-address] | all]
```

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- The MAC-to-VLAN mapping applies to all ports on the switch.
- After creating a MAC-based VLAN, be sure to configure the VLAN for selected interfaces using the `switchport allowed vlan` command.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- The binary equivalent mask matching the characters in the front of the first non-zero character must all be 1s (e.g., 111, i.e., it cannot be 101 or 001...). A mask for the MAC address: 00-50-6e-00-5f-b1 translated into binary:
  
  MAC: 00000000-01010000-01101110-00000000-01011111-10110001
  
  could be: 11111111-11xxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
  
  So the mask in hexadecimal for this example could be:
  
  ff-fx-xx-xx-xx-xx/ff-c0-00-00-00-00/ff-e0-00-00-00-00
Example
The following example assigns traffic from source MAC address 00-00-00-11-22-33 to VLAN 10.

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

**Example**
The following example displays all configured MAC address-based VLANs.

```
Console#show mac-vlan
MAC Address        VLAN ID   Priority
-----------------  --------  --------
00-00-00-11-22-33        10         0
Console#
```

**Configuring Voice VLANs**
The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port to the Voice VLAN. Alternatively, switch ports can be manually configured.

**Table 104: Voice VLAN Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice vlan</td>
<td>Defines the Voice VLAN ID</td>
<td>GC</td>
</tr>
<tr>
<td>voice vlan aging</td>
<td>Configures the aging time for Voice VLAN ports</td>
<td>GC</td>
</tr>
<tr>
<td>voice vlan mac-address</td>
<td>Configures VoIP device MAC addresses</td>
<td>GC</td>
</tr>
<tr>
<td>switchport voice vlan</td>
<td>Sets the Voice VLAN port mode</td>
<td>IC</td>
</tr>
<tr>
<td>switchport voice vlan priority</td>
<td>Sets the VoIP traffic priority for ports</td>
<td>IC</td>
</tr>
<tr>
<td>switchport voice vlan rule</td>
<td>Sets the automatic VoIP traffic detection method for ports</td>
<td>IC</td>
</tr>
</tbody>
</table>
voice vlan

This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the no form to disable the Voice VLAN.

Syntax

voice vlan voice-vlan-id

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

◆ When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.

◆ VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.

◆ Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.

◆ The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the switchport voice vlan command.

Example

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234
Console(config)#
```
**voice vlan aging**  This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

**Syntax**

```
voice vlan aging minutes
no voice vlan
```

- Specifies the port Voice VLAN membership time out.
  
  (Range: 5-43200 minutes)

**Default Setting**

1440 minutes

**Command Mode**

Global Configuration

**Command Usage**

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

The VoIP aging time starts to count down when the OUI’s MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from the voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the voice VLAN aging time.

Note that when the `switchport voice vlan` command is set to auto mode, the remaining aging time displayed by the `show voice vlan` command will be displayed. Otherwise, if the switchport voice vlan command is disabled or set to manual mode, the remaining aging time will display “NA.”

**Example**

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000
Console(config)#
```
voice vlan mac-address

This command specifies MAC address ranges to add to the OUI Telephony list. Use the no form to remove an entry from the list.

Syntax

voice vlan mac-address mac-address mask mask-address
[description description]

no voice vlan mac-address mac-address mask mask-address

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (Format: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx; for example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Format: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx; Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

Default Setting
None

Command Mode
Global Configuration

Command Usage

◆ VoIP devices attached to the switch can be identified by the manufacturer’s Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.

◆ Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting a mask of FF-FF-FF-FF-FF specifies a single MAC address.

Example
The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-00 description A new phone
Console(config)#
```
**switchport voice vlan** This command specifies the Voice VLAN mode for ports. Use the no form to disable the Voice VLAN feature on the port.

**Syntax**

```
switchport voice vlan {manual | auto}
no switchport voice vlan
```

- **manual** - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
- **auto** - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

**Default Setting**

Disabled

**Command Mode**

Interface Configuration

**Command Usage**

- When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1AB (LLDP) using the `switchport voice vlan rule` command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the `voice vlan mac-address` command.

- All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), ensure that VLAN membership is not set to access mode using the `switchport mode` command.

**Example**

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

**switchport voice vlan priority** This command specifies a CoS priority for VoIP traffic on a port. Use the no form to restore the default priority on a port.

**Syntax**

```
switchport voice vlan priority priority-value
no switchport voice vlan priority
```

- **priority-value** - The CoS priority value. (Range: 0-6)
**Default Setting**
6

**Command Mode**
Interface Configuration

**Command Usage**
Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

**Example**
The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

**switchport voice vlan rule**
This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

**Syntax**
```
[no] switchport voice vlan rule {oui | lldp}
```
- **oui** - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.
- **lldp** - Uses LLDP to discover VoIP devices attached to the port.

**Default Setting**
OUI: Enabled
LLDP: Disabled

**Command Mode**
Interface Configuration

**Command Usage**
- When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the **voice_vlan mac-address** command). MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

- LLDP checks that the “telephone bit” in the system capability TLV is turned on. See “**LLDP Commands**” on page 673 for more information on LLDP.
Example
The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

**switchport voice vlan security**
This command enables security filtering for VoIP traffic on a port. Use the `no` form to disable filtering on a port.

**Syntax**
```
[no] switchport voice vlan security
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration

**Command Usage**
- Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list (voice vlan mac-address).

**Example**
The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

**show voice vlan**
This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

**Syntax**
```
show voice vlan {oui | status}
```
- `oui` - Displays the OUI Telephony list.
- `status` - Displays the global and port Voice VLAN settings.
**Default Setting**
None

**Command Mode**
Privileged Exec

**Command Usage**
When the `switchport voice vlan` command is set to auto mode, the remaining aging time displayed by the `show voice vlan` command will be displayed (or “Not Start” will be displayed). Otherwise, if the `switchport voice vlan` command is disabled or set to manual mode, the remaining aging time will display “NA.”

**Example**

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status      : Enabled
Voice VLAN ID          : 1234
Voice VLAN aging time  : 1440 minutes

Voice VLAN Port Summary
Port     Mode     Security Rule      Priority Remaining Age (minutes)
-------- -------- -------- --------- -------- -------------
Eth 1/ 1 Auto     Enabled  OUI              6 100
Eth 1/ 2 Disabled Disabled OUI              6 NA
Eth 1/ 3 Manual   Enabled  OUI              5 NA
Eth 1/ 4 Auto     Disabled Disabled OUI              6 Not Start
Eth 1/ 5 Disabled Disabled OUI              6 NA
Eth 1/ 6 Disabled Disabled OUI              6 NA
Eth 1/ 7 Disabled Disabled OUI              6 NA
Eth 1/ 8 Disabled Disabled OUI              6 NA
Eth 1/ 9 Disabled Disabled OUI              6 NA
Eth 1/10 Disabled Disabled OUI              6 NA

Console#show voice vlan oui
OUI Address       Mask              Description
----------------- ----------------- ------------------------------
00-12-34-56-78-9A FF-FF-00-00-00-00 old phones
00-11-22-33-44-55 FF-FF-00-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF Chris' phone

Console#
```
The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port’s high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the switch’s priority queues can be configured.

**Table 105: Priority Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority Commands (Layer 2)</td>
<td>Configures the queue mode, queue weights, and default priority for untagged frames</td>
</tr>
<tr>
<td>Priority Commands (Layer 3 and 4)</td>
<td>Sets the default priority processing method (CoS or DSCP), maps priority tags for internal processing, maps values from internal priority table to CoS values used in tagged egress packets for Layer 2 interfaces, maps internal per hop behavior to hardware queues</td>
</tr>
</tbody>
</table>

**Priority Commands (Layer 2)**

This section describes commands used to configure Layer 2 traffic priority on the switch.

**Table 106: Priority Commands (Layer 2)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>queue mode</td>
<td>Sets the queue mode to Weighted Round-Robin (WRR), strict priority, or a combination of strict and weighted queuing</td>
<td>GC</td>
</tr>
<tr>
<td>queue weight</td>
<td>Assigns round-robin weights to the priority queues</td>
<td>GC</td>
</tr>
<tr>
<td>switchport priority default</td>
<td>Sets a port priority for incoming untagged frames</td>
<td>IC</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays the administrative and operational status of an interface</td>
<td>PE</td>
</tr>
<tr>
<td>show queue mode</td>
<td>Shows the current queue mode</td>
<td>PE</td>
</tr>
<tr>
<td>show queue weight</td>
<td>Shows weights assigned to the weighted queues</td>
<td>PE</td>
</tr>
</tbody>
</table>
**queue mode**  This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Use the **no** form to restore the default value.

**Syntax**

```
queue mode {strict | wrr | strict-wrr [queue-type-list]}
```

**no queue mode**

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the `queue weight` command), and servicing each queue in a round-robin fashion.
- **strict-wrr** - Uses strict or weighted service as specified for each queue.

**queue-type-list** - Indicates if the queue is a normal or strict type. (Options: 0 indicates a normal queue, 1 indicates a strict queue)

**Default Setting**

WRR

**Command Mode**

Global Configuration

**Command Usage**

- The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queuing.

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.

- Weighted Round Robin (WRR) uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the `queue weight` command to assign weights for WRR queuing to the eight priority queues.

- If Strict and WRR mode is selected, a combination of strict and weighted service is used as specified for each queue. The queues assigned to use strict or WRR priority should be specified using the `queue-type-list` parameter.

- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.
◆ Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

◆ The specified queue mode applies to all interfaces.

Example
The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

Related Commands
queue weight (543)
show queue mode (545)

queue weight
This command assigns weights to the four class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the no form to restore the default weights.

**Syntax**
```
queue weight weight0...weight3
no queue weight
```

weight0...weight3 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1-255)

**Default Setting**
Weights 1, 2, 4, 6 are assigned to queues 0 - 3 respectively.

**Command Mode**
Global Configuration

**Command Usage**
◆ This command shares bandwidth at the egress port by defining scheduling weights for Weighted Round-Robin, or for the queuing mode that uses a combination of strict and weighted queuing.

◆ Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.
Example
The following example shows how to assign round-robin weights of 1 - 4 to the CoS priority queues 0 - 3.

```
Console(config)#queue weight 1 2 3 4
Console(config)#
```

Related Commands
queue mode (542)
show queue weight (545)

**switchport priority default**
This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

**Syntax**
```
switchport priority default default-priority-id
no switchport priority default
```

```
default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.
```

**Default Setting**
The priority is not set, and the default value for untagged frames received on the interface is zero.

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
◆ The precedence for priority mapping is IP DSCP, and then default switchport priority.

◆ The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

◆ The switch provides four priority queues for each port. It can be configured to use strict priority queuing, Weighted Round Robin (WRR), or a combination of strict and weighted queuing using the **queue mode** command. Inbound frames that do not have VLAN tags are tagged with the input port’s default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 1 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)
Example
The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

Related Commands
*show interfaces switchport (389)*

**show queue mode**  This command shows the current queue mode.

**Command Mode**
Privileged Exec

**Example**

```
Console#show queue mode

Queue Mode : Weighted Round Robin Mode
Console#
```

**show queue weight**  This command displays the weights used for the weighted queues.

**Command Mode**
Privileged Exec

**Example**

```
Console#show queue weight

<table>
<thead>
<tr>
<th>Queue ID</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

Console#
```
Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 107: Priority Commands (Layer 3 and 4)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos map cos-dscp</td>
<td>Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for internal priority processing</td>
<td>GC</td>
</tr>
<tr>
<td>qos map dscp-mutation</td>
<td>Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing</td>
<td>GC</td>
</tr>
<tr>
<td>qos map phb-queue</td>
<td>Maps internal per-hop behavior values to hardware queues</td>
<td>GC</td>
</tr>
<tr>
<td>qos map trust-mode</td>
<td>Sets QoS mapping to DSCP or CoS</td>
<td>IC</td>
</tr>
<tr>
<td>show qos map cos-dscp</td>
<td>Shows ingress CoS to internal DSCP map</td>
<td>PE</td>
</tr>
<tr>
<td>show qos map dscp-mutation</td>
<td>Shows ingress DSCP to internal DSCP map</td>
<td>PE</td>
</tr>
<tr>
<td>show qos map phb-queue</td>
<td>Shows internal per-hop behavior to hardware queue map</td>
<td>PE</td>
</tr>
<tr>
<td>show qos map trust-mode</td>
<td>Shows the QoS mapping mode</td>
<td>PE</td>
</tr>
</tbody>
</table>

* The default settings used for mapping priority values to internal DSCP values and back to the hardware queues are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings unless a queuing problem occurs with a particular application.

**qos map cos-dscp**  This command maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

**Syntax**

```
qos map cos-dscp phb drop-precedence from cos0 cfi0...cos7 cfi7
```

```
no qos map cos-dscp cos0 cfi0...cos7 cfi7
```

- **phb** - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **drop-precedence** - Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)
- **cos** - CoS value in ingress packets. (Range: 0-7)
- **cfi** - Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
**DEFAULT SETTING**

Table 108: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

<table>
<thead>
<tr>
<th>CoS</th>
<th>CFI</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>(1,0)</td>
<td>(1,0)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>(2,0)</td>
<td>(2,0)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(3,0)</td>
<td>(3,0)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(4,0)</td>
<td>(4,0)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(5,0)</td>
<td>(5,0)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>(6,0)</td>
<td>(6,0)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>(7,0)</td>
<td>(7,0)</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Command Usage**

- The default mapping of CoS to PHB values shown in Table 108 is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.

- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword “from” and then up to eight CoS/CFI paired values separated by spaces.

- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.

- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used by Random Early Detection (RED) to control traffic congestion.

- The specified mapping applies to all interfaces.

**Example**

```
Console(config)#qos map cos-dscp 0 0 from 0 1
Console(config)#
```
Chapter 19 | Class of Service Commands
Priority Commands (Layer 3 and 4)

**qos map dscp-mutation**

This command maps DSCP values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

**Syntax**

```
qos map dscp-mutation phb drop-precedence from dscp0 ... dscp7

no qos map dscp-mutation dscp0 ... dscp7
```

*phb* - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

*drop-precedence* - Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

*dscp* - DSCP value in ingress packets. (Range: 0-63)

**DEFAULT SETTING.**

**Table 109: Default Mapping of DSCP Values to Internal PHB/Drop Values**

<table>
<thead>
<tr>
<th>ingress-dscp1</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>ingress-dscp10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0,0,0,0,0,0,0,0,0</td>
<td>0,0,1,0,0,0,0,0,0</td>
<td>0,0,3,0,0,0,0,0,0</td>
<td>0,1,0,0,0,0,0,0,0</td>
<td>0,0,3,0,0,0,0,0,0</td>
<td>1,0,0,0,0,0,0,0,0</td>
<td>1,1,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1,0,1,3,1,0,1,0,1</td>
<td>1,0,0,1,0,0,0,0,0</td>
<td>1,0,3,0,0,0,0,0,0</td>
<td>1,3,0,0,0,0,0,0,0</td>
<td>2,0,0,0,0,0,0,0,0</td>
<td>2,0,0,0,0,0,0,0,0</td>
<td>2,3,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2,0,2,1,2,0,2,3,3</td>
<td>2,3,0,2,0,0,0,0,0</td>
<td>3,0,3,0,0,0,0,0,0</td>
<td>3,1,0,0,0,0,0,0,0</td>
<td>3,0,3,0,0,0,0,0,0</td>
<td>3,0,3,0,0,0,0,0,0</td>
<td>3,1,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3,0,3,3,4,0,4,1,4</td>
<td>3,0,0,3,3,0,0,0,0</td>
<td>4,0,4,0,0,0,0,0,0</td>
<td>4,3,0,0,0,0,0,0,0</td>
<td>4,0,4,0,0,0,0,0,0</td>
<td>4,1,0,0,0,0,0,0,0</td>
<td>4,3,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5,0,5,1,5,0,5,3,5</td>
<td>5,0,0,5,1,0,0,0,0</td>
<td>6,0,6,0,0,0,0,0,0</td>
<td>5,1,0,0,0,0,0,0,0</td>
<td>6,0,6,0,0,0,0,0,0</td>
<td>6,0,6,0,0,0,0,0,0</td>
<td>6,1,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6,0,6,3,6,0,6,1,6</td>
<td>6,0,0,6,3,0,0,0,0</td>
<td>7,0,7,0,0,0,0,0,0</td>
<td>6,3,0,0,0,0,0,0,0</td>
<td>7,0,7,0,0,0,0,0,0</td>
<td>7,0,7,0,0,0,0,0,0</td>
<td>7,3,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>7,0,7,1,7,0,7,1,7</td>
<td>7,1,0,7,0,0,0,0,0</td>
<td>7,0,7,0,0,0,0,0,0</td>
<td>7,3,0,0,0,0,0,0,0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table. The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

**Command Mode**

Global Configuration

**Command Usage**

- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword “from” and then up to eight DSCP values separated by spaces.

- This map is only used when the QoS mapping mode is set to “DSCP” by the **qos map trust-mode** command, and the ingress packet type is IPv4.
◆ Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

◆ The specified mapping applies to all interfaces.

Example
This example changes the priority for all packets entering port 1 which contain a DSCP value of 1 to a per-hop behavior of 3 and a drop precedence of 1. Referring to Table 109, note that the DSCP value for these packets is now set to 25 (3x2^3+1) and passed on to the egress interface.

```
Console(config)#qos map dscp-mutation 3 1 from 1
Console(config)#
```

qos map phb-queue
This command determines the hardware output queues to use based on the internal per-hop behavior value. Use the no form to restore the default settings.

Syntax

```plaintext
qos map phb-queue queue-id from phb0 ... phb7
no map phb-queue phb0 ... phb7
```

- `phb` - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- `queue-id` - The ID of the priority queue. (Range: 0-7, where 7 is the highest priority queue)

**DEFAULT SETTING**

**Table 110: Mapping Internal Per-hop Behavior to Hardware Queues**

<table>
<thead>
<tr>
<th>Per-hop Behavior</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Queues</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Command Usage**

◆ Enter a queue identifier, followed by the keyword “from” and then up to eight internal per-hop behavior values separated by spaces.

◆ Egress packets are placed into the hardware queues according to the mapping defined by this command.

◆ The specified mapping applies to all interfaces.
qos map trust-mode

This command sets QoS mapping to DSCP or CoS. Use the no form to restore the default setting.

Syntax

qos map trust-mode {dscp | cos}

no qos map trust-mode

dscp - Sets the QoS mapping mode to DSCP.
cos - Sets the QoS mapping mode to CoS.

Default Setting

COS

Command Mode

Interface Configuration (Port)

Command Usage

◆ If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.

◆ If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet’s CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see page 544) is used for priority processing.

◆ If the QoS mapping mode is set to CoS with this command, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

For an untagged packet, the default port priority (see page 544) is used for priority processing.

Example

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

```
Console(config)#interface 1/1
Console(config-if)#qos map trust-mode cos
Console(config-if)#
```
**show qos map cos-dscp**  
This command shows ingress CoS/CFI to internal DSCP map.

**Syntax**

```
show qos map cos-dscp
```

**Command Mode**

Privileged Exec

**Example**

```
Console#show qos map cos-dscp
Cos Information
CoS-DSCP Map. (x,y),x: phb,y: drop precedence:
CoS : CFI  0          1
---------------------------------
0            (0,0)     (0,0)
1            (1,0)     (1,0)
2            (2,0)     (2,0)
3            (3,0)     (3,0)
4            (4,0)     (4,0)
5            (5,0)     (5,0)
6            (6,0)     (6,0)
7            (7,0)     (7,0)
Console#
```

**show qos map dscp-mutation**  
This command shows the ingress DSCP to internal DSCP map.

**Syntax**

```
show qos map dscp-mutation
```

**Command Mode**

Privileged Exec

**Command Usage**

This map is only used when the QoS mapping mode is set to “DSCP” by the `qos map trust-mode` command, and the ingress packet type is IPv4.

**Example**

The ingress DSCP is composed of “d1” (most significant digit in the left column) and “d2” (least significant digit in the top row (in other words, ingress DSCP = d1 * 10 + d2); and the corresponding internal DSCP and drop precedence is shown at the intersecting cell in the table.

```
Console#show qos map dscp-mutation
Information of global DSCP mutation map. (x,y),x: PHB,y: drop precedence:
d1: d2  0 1 2 3 4 5 6 7 8 9
------------------------------------------
0 :   (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)
1 :   (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)
2 :   (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)
3 :   (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)
```

---

- 551 -
Chapter 19 | Class of Service Commands
Priority Commands (Layer 3 and 4)

Priority Commands (Layer 3 and 4)

This command shows internal per-hop behavior to hardware queue map.

Syntax

```
show qos map phb-queue
```

Command Mode
Privileged Exec

Example

```
Console#show qos map phb-queue
PHB Queue Map:
PHB: 0 1 2 3 4 5 6 7
-----
Queue: 1 0 0 1 2 2 3 3
Console#
```

This command shows the QoS mapping mode.

Syntax

```
show qos map trust-mode interface interface
```

```
interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)
```

Command Mode
Privileged Exec

Example

The following shows that the trust mode is set to CoS:

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
CoS Map mode: CoS mode
Console#
```
Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 111: Quality of Service Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map</td>
<td>Creates a class map for a type of traffic</td>
<td>GC</td>
</tr>
<tr>
<td>description</td>
<td>Specifies the description of a class map</td>
<td>CM</td>
</tr>
<tr>
<td>match</td>
<td>Defines the criteria used to classify traffic</td>
<td>CM</td>
</tr>
<tr>
<td>rename</td>
<td>Redefines the name of a class map</td>
<td>CM</td>
</tr>
<tr>
<td>policy-map</td>
<td>Creates a policy map for multiple interfaces</td>
<td>GC</td>
</tr>
<tr>
<td>description</td>
<td>Specifies the description of a policy map</td>
<td>PM</td>
</tr>
<tr>
<td>class</td>
<td>Defines a traffic classification for the policy to act on</td>
<td>PM</td>
</tr>
<tr>
<td>rename</td>
<td>Redefines the name of a policy map</td>
<td>PM</td>
</tr>
<tr>
<td>police flow</td>
<td>Defines an enforcer for classified traffic based on a metered flow rate</td>
<td>PM-C</td>
</tr>
<tr>
<td>police srtcm-color</td>
<td>Defines an enforcer for classified traffic based on a single rate three color meter</td>
<td>PM-C</td>
</tr>
<tr>
<td>police trtc-m-color</td>
<td>Defines an enforcer for classified traffic based on a two rate three color meter</td>
<td>PM-C</td>
</tr>
<tr>
<td>set cos</td>
<td>Services IP traffic by setting a class of service value for matching packets for internal processing</td>
<td>PM-C</td>
</tr>
<tr>
<td>set ip dscp</td>
<td>Services IP traffic by setting an IP DSCP value for matching packets for internal processing</td>
<td>PM-C</td>
</tr>
<tr>
<td>set phb</td>
<td>Services IP traffic by setting a per-hop behavior value for matching packets for internal processing</td>
<td>PM-C</td>
</tr>
<tr>
<td>service-policy</td>
<td>Applies a policy map defined by the policy-map command to the input of a particular interface</td>
<td>IC</td>
</tr>
<tr>
<td>show class-map</td>
<td>Displays the QoS class maps which define matching criteria used for classifying traffic</td>
<td>PE</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations</td>
<td>PE</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays the configuration of all classes configured for all service policies on the specified interface</td>
<td>PE</td>
</tr>
</tbody>
</table>
To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the `class-map` command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.

2. Use the `match` command to select a specific type of traffic based on an access list, an IPv4 DSCP value, IPv4 Precedence value, IPv6 DSCP value, a VLAN, or a CoS value. Note that a class map can include match settings for both IP values and a VLAN.

3. Use the `policy-map` command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.

4. Use the `class` command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain up to 200 class maps.

5. Use the `set phb`, `set cos` or `set ip dscp` command to modify the per-hop behavior, the class of service value in the VLAN tag, or the priority bits in the IP header (IP DSCP value) for the matching traffic class, and use one of the `police` commands to monitor parameters such as the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.

6. Use the `service-policy` command to assign a policy map to a specific interface.

**Note:** Create a Class Map before creating a Policy Map.

class-map  This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the `no` form to delete a class map.

**Syntax**

```markdown
[no] class-map class-map-name [match-all | match-any]
```

class-map-name - Name of the class map. (Range: 1-32 characters)

match-all - Match all conditions within a class map.

match-any - Match any condition within a class map.

**Default Setting**

None

**Command Mode**

Global Configuration
Command Usage

◆ First enter this command to designate a class map and enter the Class Map configuration mode. Then use match commands to specify the criteria for ingress traffic that will be classified under this class map.

◆ One or more class maps can be assigned to a policy map (page 557). The policy map is then bound by a service policy to an interface (page 568). A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the match or set commands.

Example

This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

Related Commands

show class-map (569)

description

This command specifies the description of a class map or policy map.

Syntax

description string

string - Description of the class map or policy map. (Range: 1-64 characters)

Command Mode

Class Map Configuration
Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description “matches packets marked for DSCP service value 3”
Console(config-cmap)#
```
match  This command defines the criteria used to classify traffic. Use the `no` form to delete the matching criteria.

Syntax

```plaintext
[no] match (access-list acl-name | cos cos | ip dscp dscp | ip precedence ip-precedence | ipv6 dscp dscp | vlan vlan)
```

- `acl-name` - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- `cos` - A Class of Service value. (Range: 0-7)
- `dscp` - A Differentiated Service Code Point value. (Range: 0-63)
- `ip-precedence` - An IP Precedence value. (Range: 0-7)
- `interface`
  - `unit/port`  
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)
- `vlan-id` - A VLAN. (Range: 1-4094)

Default Setting
None

Command Mode
Class Map Configuration

Command Usage
◆ First enter the `class-map` command to designate a class map and enter the Class Map configuration mode. Then use `match` commands to specify the fields within ingress packets that must match to qualify for this class map.
◆ If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
◆ A class map may include any combination of an
◆ Up to 16 match entries can be included in a class map.

Example
This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

```plaintext
Console(config)#class-map rd-class#1 match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```
This example creates a class map call “rd-class#2,” and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call “rd-class#3,” and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

**rename**  This command redefines the name of a class map or policy map.

**Syntax**

```
rename map-name
```

- *map-name* - Name of the class map or policy map. (Range: 1-32 characters)

**Command Mode**

Class Map Configuration
Policy Map Configuration

**Example**

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

**policy-map**  This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

**Syntax**

```
[no] policy-map policy-map-name
```

- *policy-map-name* - Name of the policy map. (Range: 1-32 characters)

**Default Setting**

None

**Command Mode**

Global Configuration
Command Usage

◆ Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches the criteria defined in a class map.

◆ A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command.

◆ Create a Class Map (page 557) before assigning it to a Policy Map.

Example
This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#
```

class
This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

Syntax

```
[no] class class-map-name
```

*class-map-name* - Name of the class map. (Range: 1-32 characters)

Default Setting
None

Command Mode
Policy Map Configuration

Command Usage

◆ Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** command and one of the **police** commands to specify the match criteria, where the:

- **set phb** command sets the per-hop behavior value in matching packets. (This modifies packet priority for internal processing only.)
- **set cos** command sets the class of service value in matching packets.
  (This modifies packet priority in the VLAN tag.)

- **set ip dscp** command sets the IP DSCP value in matching packets.
  (This modifies packet priority in the IP header.)

- **police** commands define parameters such as the maximum throughput, burst rate, and response to non-conforming traffic.

  - Up to 200 classes can be included in a policy map.

**Example**

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set phb** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4,000 bytes, and configure the response to drop any violating packets.

```console
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
    violate-action drop
Console(config-pmap-c)#
```

**police flow** This command defines an enforcer for classified traffic based on the metered flow rate. Use the no form to remove a policer.

**Syntax**

```plaintext
[no] police flow committed-rate committed-burst
    conform-action transmit
    violate-action (drop|new-dscp)
```

- **committed-rate** - Committed information rate (CIR) in kilobits per second.
  (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

- **committed-burst** - Committed burst size (BC) in bytes.
  (Range: 0-16000000 at a granularity of 4k bytes)

- **conform-action** - Action to take when packet is within the CIR and BC.
  (There are enough tokens to service the packet, the packet is set green).

- **violate-action** - Action to take when packet exceeds the CIR and BC.
  (There are not enough tokens to service the packet, the packet is set red).

- **transmit** - Transmits without taking any action.

- **drop** - Drops packet as required by violate-action.

- **new-dscp** - Differentiated Service Code Point (DSCP) value. (Range: 0-63)
Default Setting
None

Command Mode
Policy Map Class Configuration

Command Usage
◆ You can configure up to 200 policers (i.e., class maps) for ingress ports.

◆ The **committed-rate** cannot exceed the configured interface speed, and the **committed-burst** cannot exceed 16 Mbytes.

◆ Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the **committed-burst** field, and the average rate tokens are added to the bucket is by specified by the **committed-rate** option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.

◆ The behavior of the meter is specified in terms of one token bucket \( C \), the rate at which the tokens are incremented \( \text{CIR} \) – Committed Information Rate, and the maximum size of the token bucket \( \text{BC} \) – Committed Burst Size.

The token bucket \( C \) is initially full, that is, the token count \( T_c(0) = \text{BC} \). Thereafter, the token count \( T_c \) is updated \( \text{CIR} \) times per second as follows:

- If \( T_c \) is less than \( \text{BC} \), \( T_c \) is incremented by one, else
- \( T_c \) is not incremented.

When a packet of size \( B \) bytes arrives at time \( t \), the following happens:

- If \( T_c(t) - B \geq 0 \), the packet is green and \( T_c \) is decremented by \( B \) down to the minimum value of 0, else
- else the packet is red and \( T_c \) is not decremented.

Example
This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set phb** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
violating-action drop
Console(config-pmap-c)#
```
police srtcm-color  This command defines an enforcer for classified traffic based on a single rate three color meter (srTCM). Use the no form to remove a policer.

Syntax

[no] police {srtcm-color-blind | srtcm-color-aware}

- committed-rate committed-burst excess-burst
- conform-action transmit
- exceed-action {drop | new-dscp}
- violate action {drop | new-dscp}

srtcm-color-blind - Single rate three color meter in color-blind mode.

srtcm-color-aware - Single rate three color meter in color-aware mode.

- committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

- committed-burst - Committed burst size (BC) in bytes. (Range: 0-1600000 at a granularity of 4k bytes)

- excess-burst - Excess burst size (BE) in bytes. (Range: 0-1600000 at a granularity of 4k bytes)

- conform-action - Action to take when rate is within the CIR and BC. (There are enough tokens in bucket BC to service the packet, packet is set green).

- exceed-action - Action to take when rate exceeds the CIR and BC but is within the BE. (There are enough tokens in bucket BE to service the packet, the packet is set yellow.)

- violate-action - Action to take when rate exceeds the BE. (There are not enough tokens in bucket BE to service the packet, the packet is set red.)

- transmit - Transmits without taking any action.

- drop - Drops packet as required by exceed-action or violate-action.

- new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Setting
None

Command Mode
Policy Map Class Configuration

Command Usage
* You can configure up to 200 policers (i.e., class maps) for ingress ports.

* The committed-rate cannot exceed the configured interface speed, and the committed-burst and excess-burst cannot exceed 16 Mbytes.

* The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – Committed Information Rate (CIR), Committed Burst Size (BC), and Excess Burst Size (BE).
◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green if it doesn't exceed the CIR and BC, yellow if it does exceed the CIR and BC, but not the BE, and red otherwise.

◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

◆ The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

- If Tc is less than BC, Tc is incremented by one, else
- if Te is less then BE, Te is incremented by one, else
- neither Tc nor Te is incremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode:

- If Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0,
- else the packet is red and neither Tc nor Te is decremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode:

- If the packet has been precolored as green and Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if
- Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

**Example**

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the set phb command to classify the service that incoming packets will receive, and then uses the `police srTCM-color-blind`
command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the excess burst rate to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the excess burst size.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

**police trtcm-color** This command defines an enforcer for classified traffic based on a two rate three color meter (trTCM). Use the no form to remove a policer.

**Syntax**

```
[no] police {trtcm-color-blind | trtcm-color-aware}
  committed-rate committed-burst peak-rate peak-burst
  conform-action transmit
  exceed-action {drop | new-dscp}
  violate action {drop | new-dscp}

trtcm-color-blind - Two rate three color meter in color-blind mode.

trtcm-color-aware - Two rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second.
(Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes.
(Range: 0-16000000 at a granularity of 4k bytes)

peak-rate - Peak information rate (PIR) in kilobits per second.
(Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

peak-burst - Peak burst size (BP) in bytes.
(Range: 0-16000000 at a granularity of 4k bytes)

conform-action - Action to take when rate is within the CIR and BP. (Packet size does not exceed BP and there are enough tokens in bucket BC to service the packet, the packet is set green.)

exceed-action - Action to take when rate exceeds the CIR but is within the PIR. (Packet size exceeds BC but there are enough tokens in bucket BP to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the PIR. (There are not enough tokens in bucket BP to service the packet, the packet is set red.)

drop - Drops packet as required by exceed-action or violate-action.

transmit - Transmits without taking any action.
new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

**Default Setting**
None

**Command Mode**
Policy Map Class Configuration

**Command Usage**
- You can configure up to 200 policers (i.e., class maps) for ingress ports.
- The *committed-rate* and *peak-rate* cannot exceed the configured interface speed, and the *committed-burst* and *peak-burst* cannot exceed 16 Mbytes.
- The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – Committed Information Rate (CIR) and Peak Information Rate (PIR), and their associated burst sizes - Committed Burst Size (BC) and Peak Burst Size (BP).
- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn’t exceed the CIR.

The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.
- The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:
- If Tp(t)-B < 0, the packet is red, else
- if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.
When a packet of size $B$ bytes arrives at time $t$, the following happens if trTCM is configured to operate in color-aware mode:

- If the packet has been precolored as red or if $T_p(t) - B < 0$, the packet is red, else
- if the packet has been precolored as yellow or if $T_c(t) - B < 0$, the packet is yellow and $T_p$ is decremented by $B$, else
- the packet is green and both $T_p$ and $T_c$ are decremented by $B$.

The trTCM can be used to mark an IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

**Example**

This example creates a policy called “rd-policy,” uses the `class` command to specify the previously defined “rd-class,” uses the `set phb` command to classify the service that incoming packets will receive, and then uses the `police trtcm-color-blind` command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```console
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police trtcm-color-blind 100000 4000 1000000 6000 conform-action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

**set cos**

This command modifies the class of service (CoS) value for a matching packet (as specified by the `match` command) in the packet’s VLAN tag. Use the `no` form to remove this setting.

**Syntax**

```
[no] set cos cos-value
```

`cos-value` - Class of Service value. (Range: 0-7)

**Default Setting**

None

**Command Mode**

Policy Map Class Configuration

**Command Usage**

- The `set cos` command is used to set the CoS value in the VLAN tag for matching packets.
The `set cos` and `set phb` command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

**Example**
This example creates a policy called “rd-policy,” uses the `class` command to specify the previously defined “rd-class,” uses the `set cos` command to classify the service that incoming packets will receive, and then uses the `police flow` command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```plaintext
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
                         violate-action drop
Console(config-pmap-c)#
```

**set ip dscp** This command modifies the IP DSCP value in a matching packet (as specified by the `match` command). Use the `no` form to remove this traffic classification.

**Syntax**

```plaintext
[no] set ip dscp new-dscp
```

- `new-dscp` - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)

**Default Setting**
None

**Command Mode**
Policy Map Class Configuration

**Command Usage**
The `set ip dscp` command is used to set the priority values in the packet’s ToS field for matching packets.
Example
This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the set ip dscp command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#
```

set phb  This command services IP traffic by setting a per-hop behavior value for a matching packet (as specified by the match command) for internal processing. Use the no form to remove this setting.

Syntax

```
[no] set phb phb-value
```

- `phb-value` - Per-hop behavior value. (Range: 0-7)

Default Setting
None

Command Mode
Policy Map Class Configuration

Command Usage

- The set phb command is used to set an internal QoS value in hardware for matching packets (see Table 109, "Default Mapping of DSCP Values to Internal PHB/Drop Values"). The QoS label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion by the police srtcm-color command and police trtc-color command.

- The set cos and set phb command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.
Example
This example creates a policy called “rd-policy,” uses the class command to specify
the previously defined “rd-class,” uses the set phb command to classify the service
that incoming packets will receive, and then uses the police flow command to limit
the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure
the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

service-policy This command applies a policy map defined by the policy-map command to the
ingress side of a particular interface. Use the no form to remove this mapping.

Syntax

```
[no] service-policy input policy-map-name
input - Apply to the input traffic.
policy-map-name - Name of the policy map for this interface.
(Range: 1-32 characters)
```

Default Setting
No policy map is attached to an interface.

Command Mode
Interface Configuration (Ethernet)

Command Usage
◆ Only one policy map can be assigned to an interface.
◆ First define a class map, then define a policy map, and finally use the service-
policy command to bind the policy map to the required interface.
◆ The switch does not allow a policy map to be bound to an interface for egress
traffic.

Example
This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```
**show class-map**  This command displays the QoS class maps which define matching criteria used for classifying traffic.

**Syntax**

```
show class-map [class-map-name]
```

*class-map-name* - Name of the class map. (Range: 1-32 characters)

**Default Setting**
Displays all class maps.

**Command Mode**
Privileged Exec

**Example**

```
Console#show class-map
Class Map match-any rd-class#1
  Description:
    Match ip dscp 10
    Match access-list rd-access
    Match ip dscp 0

Class Map match-any rd-class#2
  Match ip precedence 5

Class Map match-any rd-class#3
  Match vlan 1

Console#
```

**show policy-map**  This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

**Syntax**

```
show policy-map [policy-map-name [class class-map-name]]
```

*policy-map-name* - Name of the policy map. (Range: 1-32 characters)

*class-map-name* - Name of the class map. (Range: 1-32 characters)

**Default Setting**
Displays all policy maps and all classes.

**Command Mode**
Privileged Exec
Example

```
  Console#show policy-map
  Policy Map rd-policy
  Description:
  class rd-class
  set PHB 3
  Console#show policy-map rd-policy class rd-class
  Policy Map rd-policy
  class rd-class
  set PHB 3
  Console#
```

**show policy-map interface**

This command displays the service policy assigned to the specified interface.

**Syntax**

```
  show policy-map interface interface input

  interface
  unit/port

  unit - Unit identifier. (Range: 1)
  port - Port number. (Range: 1-28/52)
```

**Command Mode**

Privileged Exec

**Example**

```
  Console#show policy-map interface 1/5 input
  Service-policy rd-policy
  Console#
```
Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to check for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 112: Multicast Filtering Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping</td>
<td>Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, enables proxy reporting, displays current snooping settings, and displays the multicast service and group members</td>
</tr>
<tr>
<td>Static Multicast Routing</td>
<td>Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs</td>
</tr>
<tr>
<td>IGMP Filtering and Throttling</td>
<td>Configures IGMP filtering and throttling</td>
</tr>
<tr>
<td>MLD Snooping</td>
<td>Configures multicast snooping for IPv6</td>
</tr>
<tr>
<td>MLD Filtering and Throttling</td>
<td>Configures MLD filtering and throttling for IPv6.</td>
</tr>
<tr>
<td>Multicast VLAN Registration for IPv4</td>
<td>Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic</td>
</tr>
<tr>
<td>Multicast VLAN Registration for IPv6</td>
<td>Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic</td>
</tr>
</tbody>
</table>
IGMP Snooping

This section describes commands used to configure IGMP snooping on the switch.

Table 113: IGMP Snooping Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>Enables IGMP snooping</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping priority</td>
<td>Assigns a priority to all multicast traffic</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping proxy-reporting</td>
<td>Enables IGMP Snooping with Proxy Reporting</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping querier</td>
<td>Allows this device to act as the querier for IGMP snooping</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping router-alert-option-check</td>
<td>Discards any IGMPv2/v3 packets that do not include the Router Alert option</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping router-port-expire-time</td>
<td>Configures the querier timeout</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping tcn-flood</td>
<td>Floods multicast traffic when a Spanning Tree topology change occurs</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping tcn-query-solicit</td>
<td>Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping unregistered-data-flood</td>
<td>Floods unregistered multicast traffic into the attached VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping unsolicited-report-interval</td>
<td>Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping version</td>
<td>Configures the IGMP version for snooping</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping version-exclusive</td>
<td>Discards received IGMP messages which use a version different to that currently configured</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan general-query-suppression</td>
<td>Suppresses general queries except for ports attached to downstream multicast hosts</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan immediate-leave</td>
<td>Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan last-memb-query-count</td>
<td>Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan last-memb-query-intvl</td>
<td>Configures the last-member-query interval</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan mrd</td>
<td>Sends multicast router solicitation messages</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan proxy-address</td>
<td>Configures a static address for proxy IGMP query and reporting</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan proxy-reporting</td>
<td>Enables IGMP Snooping with Proxy Reporting</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan query-interval</td>
<td>Configures the interval between sending IGMP proxy general queries</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp snooping vlan query-resp-intvl</td>
<td>Configures the maximum time the system waits for a response to proxy general queries</td>
<td>GC</td>
</tr>
</tbody>
</table>
### Table 113: IGMP Snooping Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip igmp snooping vlan static</strong></td>
<td>Adds an interface as a member of a multicast group</td>
<td>GC</td>
</tr>
<tr>
<td><strong>ip igmp snooping vlan version</strong></td>
<td>Configures the IGMP version for snooping</td>
<td>GC</td>
</tr>
<tr>
<td><strong>ip igmp snooping vlan version-exclusive</strong></td>
<td>Discards received IGMP messages which use a version different to that currently configured</td>
<td>GC</td>
</tr>
<tr>
<td><strong>clear ip igmp snooping groups dynamic</strong></td>
<td>Clears multicast group information dynamically learned through IGMP snooping</td>
<td>PE</td>
</tr>
<tr>
<td><strong>clear ip igmp snooping statistics</strong></td>
<td>Clears IGMP snooping statistics</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show ip igmp snooping</strong></td>
<td>Shows the IGMP snooping, proxy, and query configuration</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show ip igmp snooping group</strong></td>
<td>Shows known multicast group, source, and host port mapping</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show ip igmp snooping mrouter</strong></td>
<td>Shows multicast router ports</td>
<td>PE</td>
</tr>
<tr>
<td><strong>show ip igmp snooping statistics</strong></td>
<td>Shows IGMP snooping protocol statistics for the specified interface</td>
<td>PE</td>
</tr>
</tbody>
</table>

---

**ip igmp snooping**  
This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the **no** form to disable it.

**Syntax**

```
[no] ip igmp snooping [vlan vlan-id]

vlan-id - VLAN ID (Range: 1-4094)
```

**Default Setting**  
Enabled

**Command Mode**  
Global Configuration

**Command Usage**

- When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.

- When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
Example
The following example enables IGMP snooping globally.

```
Console(config)#ip igmp snooping
Console(config)#
```

**ip igmp snooping priority**  This command assigns a priority to all multicast traffic. Use the **no** form to restore the default setting.

**Syntax**

```
ip igmp snooping priority priority
no ip igmp snooping priority
```

- **priority** - The CoS priority assigned to all multicast traffic. (Range: 0-7, where 7 is the highest priority)

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

**Example**

```
Console(config)#ip igmp snooping priority 6
Console(config)#
```

**Related Commands**
show ip igmp snooping (589)

**ip igmp snooping proxy-reporting**  This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

**Syntax**

```
[no] ip igmp snooping proxy-reporting
ip igmp snooping vlan vlan-id proxy-reporting {enable | disable}
no ip igmp snooping vlan vlan-id proxy-reporting
```

- **vlan-id** - VLAN ID (Range: 1-4094)
**enable** - Enable on the specified VLAN.

**disable** - Disable on the specified VLAN.

**Default Setting**
Global: Disabled
VLAN: Based on global setting

**Command Mode**
Global Configuration

**Command Usage**
- When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

- If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

**Example**

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

**ip igmp snooping querier**
This command enables the switch as an IGMP querier. Use the **no** form to disable it.

**Syntax**

```
[no] ip igmp snooping querier
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

**Example**

```
Console(config)#ip igmp snooping querier
Console(config)#
```
**ip igmp snooping router-alert-option-check**

This command-discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the `no` form to ignore the Router Alert Option when receiving IGMP messages.

**Syntax**

```
[no] ip igmp snooping router-alert-option-check
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

**Example**

```console
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

**ip igmp snooping router-port-expire-time**

This command configures the querier time out. Use the `no` form to restore the default.

**Syntax**

```
ip igmp snooping router-port-expire-time seconds
no ip igmp snooping router-port-expire-time
```

- `seconds` - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535; Recommended Range: 300-500)

**Default Setting**

300 seconds

**Command Mode**

Global Configuration
Example
The following shows how to configure the time out to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

**ip igmp snooping tcn-flood**

This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable flooding.

**Syntax**

```
[no] ip igmp snooping tcn-flood
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

◆ When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into “multicast flooding mode” for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

◆ If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a time out mechanism is used to delete all of the currently learned multicast channels.

◆ When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.

◆ By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.

◆ When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.
The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

**Example**
The following example enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

**ip igmp snooping tcn-query-solicit**
This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the no form to disable this feature.

**Syntax**

```
[no] ip igmp snooping tcn-query-solicit
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**

- When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it will also immediately issues an IGMP general query.

- The **ip igmp snooping tcn query-solicit** command can be used to send a query solicitation whenever it notices a topology change, even if the switch is not the root bridge in the spanning tree.

**Example**
The following example instructs the switch to issue an IGMP general query whenever it receives a spanning tree topology change notification.

```
Console(config)#ip igmp snooping tcn query-solicit
Console(config)#
```
**ip igmp snooping unregistered-data-flood**

This command floods unregistered multicast traffic into the attached VLAN. Use the `no` form to drop unregistered multicast traffic.

**Syntax**

```
[no] ip igmp snooping unregistered-data-flood
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

**Example**

```
Console(config)#ip igmp snooping unregistered-data-flood
Console(config)#
```

---

**ip igmp snooping unsolicited-report-interval**

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the `no` form to restore the default value.

**Syntax**

```
ip igmp snooping unsolicited-report-interval seconds
no ip igmp snooping unsolicited-report-interval
```

- `seconds` - The interval at which to issue unsolicited reports.
  (Range: 1-65535 seconds)

**Default Setting**

400 seconds

**Command Mode**

Global Configuration

**Command Usage**

- When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.

- This command only applies when proxy reporting is enabled (see page 574).
### ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

#### Syntax

```
ip igmp snooping [vlan vlan-id] version {1 | 2 | 3}
no ip igmp snooping version
```

* **vlan-id** - VLAN ID (Range: 1-4094)
* **1** - IGMP Version 1
* **2** - IGMP Version 2
* **3** - IGMP Version 3

#### Default Setting

- **Global**: IGMP Version 2
- **VLAN**: Not configured, based on global setting

#### Command Mode

Global Configuration

#### Command Usage

- This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

#### Example

The following configures the global setting for IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```
**ip igmp snooping version-exclusive**

This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the **ip igmp snooping version** command. Use the **no** form to disable this feature.

**Syntax**

```
ip igmp snooping [vlan vlan-id] version-exclusive
no ip igmp snooping version-exclusive
```

*vlan-id* - VLAN ID (Range: 1-4094)

**Default Setting**

Global: Disabled
VLAN: Disabled

**Command Mode**

Global Configuration

**Command Usage**

- If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- When this function is disabled, the currently selected version is backward compatible (see the **ip igmp snooping version** command.

**Example**

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```

**ip igmp snooping vlan general-query-suppression**

This command suppresses general queries except for ports attached to downstream multicast hosts. Use the **no** form to flood general queries to all ports except for the multicast router port.

**Syntax**

```
[no] ip igmp snooping vlan vlan-id general-query-suppression
```

*vlan-id* - VLAN ID (Range: 1-4094)

**Default Setting**

Disabled

**Command Mode**

Global Configuration
**Command Usage**

- By default, general query messages are flooded to all ports, except for the multicast router through which they are received.

- If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

**Example**

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

**ip igmp snooping vlan immediate-leave**

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

**Syntax**

```
[no] ip igmp snooping vlan vlan-id immediate-leave
```

- **vlan-id** - VLAN ID (Range: 1-4094)

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- If immediate-leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the time out period. (The time out for this release is currently defined by **Last Member Query Interval** (fixed at one second) * **Robustness Variable** (fixed at 2) as defined in RFC 2236.

- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.
**Example**
The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

**ip igmp snooping vlan last-memb-query-count**
This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the `no` form to restore the default.

**Syntax**
```
ip igmp snooping vlan vlan-id last-memb-query-count count
no ip igmp snooping vlan vlan-id last-memb-query-count
```

- `vlan-id` - VLAN ID (Range: 1-4094)
- `count` - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

**Default Setting**
2

**Command Mode**
Global Configuration

**Command Usage**
This command will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled (page 574).

**Example**
```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

**ip igmp snooping vlan last-memb-query-intvl**
This command configures the last-member-query interval. Use the `no` form to restore the default.

**Syntax**
```
ip igmp snooping vlan vlan-id last-memb-query-intvl interval
no ip igmp snooping vlan vlan-id last-memb-query-intvl
```

- `vlan-id` - VLAN ID (Range: 1-4094)
- `interval` - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)
**Default Setting**
10 (1 second)

**Command Mode**
Global Configuration

**Command Usage**
◆ When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.

◆ A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.

◆ This command will take effect only if IGMP snooping proxy reporting is enabled (page 574).

**Example**

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

**ip igmp snooping vlan mrd**
This command enables sending of multicast router solicitation messages. Use the **no** form to disable these messages.

**Syntax**

```
[no] ip igmp snooping vlan vlan-id mrd
```

`vlan-id` - VLAN ID (Range: 1-4094)

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
◆ Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.
Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router’s start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the `no ip igmp snooping vlan mrd` command.

This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

**Example**

This example disables sending of multicast router solicitation messages on VLAN 1.

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

**ip igmp snooping vlan proxy-address**

This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the `no` form to restore the default source address.

**Syntax**

```
[no] ip igmp snooping vlan vlan-id proxy-address source-address
```

- `vlan-id` - VLAN ID (Range: 1-4094)
- `source-address` - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

**Default Setting**

0.0.0.0

**Command Mode**

Global Configuration

**Command Usage**

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.
To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

**Rules Used for Proxy Reporting**

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.

- If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

**Example**

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

**ip igmp snooping vlan query-interval**

This command configures the interval between sending IGMP general queries. Use the no form to restore the default.

**Syntax**

```
ip igmp snooping vlan vlan-id query-interval interval
no ip igmp snooping vlan vlan-id query-interval
```

- `vlan-id` - VLAN ID (Range: 1-4094)
- `interval` - The interval between sending IGMP general queries. (Range: 2-31744 seconds)

**Default Setting**

125 seconds

**Command Mode**

Global Configuration
Command Usage

- An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.

- This command applies when the switch is serving as the querier (page 575), or as a proxy host when IGMP snooping proxy reporting is enabled (page 574).

Example

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

```
ip igmp snooping vlan query-resp-intvl
```

This command configures the maximum time the system waits for a response to general queries. Use the no form to restore the default.

Syntax

```
  ip igmp snooping vlan vlan-id query-resp-intvl interval

  no ip igmp snooping vlan vlan-id query-resp-intvl
```

```
  vlan-id - VLAN ID (Range: 1-4094)

  interval - The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second)
```

Default Setting

100 (10 seconds)

Command Mode

Global Configuration

Command Usage

This command applies when the switch is serving as the querier (page 575), or as a proxy host when IGMP snooping proxy reporting is enabled (page 574).

Example

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```
**ip igmp snooping vlan static**  This command adds a port to a multicast group. Use the **no** form to remove the port.

**Syntax**

```
[no] ip igmp snooping vlan vlan-id static ip-address interface
```

- `vlan-id` - VLAN ID (Range: 1-4094)
- `ip-address` - IP address for multicast group
- `interface`
  - `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)
- `port-channel channel-id` (Range: 1-16)

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

◆ Static multicast entries are never aged out.

◆ When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

**Example**

The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

**clear ip igmp snooping groups dynamic**  This command clears multicast group information dynamically learned through IGMP snooping.

**Syntax**

```
clear ip igmp snooping groups dynamic
```

**Command Mode**

Privileged Exec

**Command Usage**

This command only clears entries learned though IGMP snooping. Statically configured multicast address are not cleared.
Example

```console
Console#clear ip igmp snooping groups dynamic
Console#
```

clear ip igmp snooping statistics

This command clears IGMP snooping statistics.

**Syntax**

```plaintext
clear ip igmp snooping statistics [interface interface]
```

`interface`

- `ethernet unit/port`
  
  `unit` - Unit identifier. (Range: 1)
  
  `port` - Port number. (Range: 1-28/52)

- `port-channel channel-id` (Range: 1-16)

- `vlan vlan-id` - VLAN identifier (Range: 1-4094)

**Command Mode**

Privileged Exec

**Example**

```console
Console#clear ip igmp snooping statistics
Console#
```

show ip igmp snooping

This command shows the IGMP snooping, proxy, and query configuration settings.

**Syntax**

```plaintext
show ip igmp snooping [vlan vlan-id]
```

`vlan-id` - VLAN ID (1-4094)

**Command Mode**

Privileged Exec

**Command Usage**

This command displays global and VLAN-specific IGMP configuration settings.

**Example**

The following shows the current IGMP snooping configuration:

```console
Console#show ip igmp snooping
IGMP Snooping : Enabled
Router Port Expire Time : 300 s
Router Alert Check : Disabled
```
show ip igmp snooping group

This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

Syntax

```
show ip igmp snooping group [host-ip-addr ip-address interface | igmpsnp | sort-by-port | user | vlan vlan-id [user | igmpsnp]]
```

- **ip-address** - IP address for multicast group
- **interface**
  - `ethernet unit/port`
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)
- **vlan-id** - VLAN ID (1-4094)
- **igmpsnp** - Display only entries learned through IGMP snooping.
- **sort-by-port** - Display entries sorted by port.
- **user** - Display only the user-configured multicast entries.
**Default Setting**  
None

**Command Mode**  
Privileged Exec

**Command Usage**  
Member types displayed include IGMP or USER, depending on selected options.

**Example**  
The following shows the multicast entries learned through IGMP snooping for VLAN 1.

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
H - Host counts (number of hosts join the group on this port).
P - Port counts (number of ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

<table>
<thead>
<tr>
<th>VLAN Group</th>
<th>Port</th>
<th>Up time</th>
<th>Expire</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 224.1.1.1</td>
<td></td>
<td>00:00:00:37</td>
<td></td>
<td>2(P)</td>
</tr>
<tr>
<td></td>
<td>Eth 1/ 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth 1/ 2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Console#
```

**show ip igmp snooping mrouter**  
This command displays information on statically configured and dynamically learned multicast router ports.

**Syntax**  
```
show ip igmp snooping mrouter [vlan vlan-id]
```

- **vlan-id** - VLAN ID (Range: 1-4094)

**Default Setting**  
Displays multicast router ports for all configured VLANs.

**Command Mode**  
Privileged Exec

**Command Usage**  
Multicast router port types displayed include Static or Dynamic.
Example
The following shows the ports in VLAN 1 which are attached to multicast routers.

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M’cast Router Ports Type    Expire
---- ------------------- ------- --------
1    Eth 1/4             Dynamic 0:4:28
1    Eth 1/10            Static
Console#
```

**show ip igmp snooping statistics**
This command shows IGMP snooping protocol statistics for the specified interface.

**Syntax**
```
show ip igmp snooping statistics
{input [interface interface] | output [interface interface] | query [vlan vlan-id]}
```

- **interface**
  - **ethernet unit/port**
    - **unit** - Unit identifier. (Range: 1)
    - **port** - Port number. (Range: 1-28/52)
  - **port-channel channel-id** (Range: 1-16)
  - **vlan vlan-id** - VLAN ID (Range: 1-4094)

- **query** - Displays IGMP snooping-related statistics.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**
The following shows IGMP protocol statistics input:

```
Console#show ip igmp snooping statistics input interface ethernet 1/1
Input Statistics:
  Interface Report  Leave  G Query  G(-S)-S Query  Drop  Join  Succ  Group
  --------- -------- -------- ------------- -------- ------ ------ -------
  Eth 1/ 1    23       11        4            10        5       14      5
Console#
```
The following shows IGMP protocol statistics output:

```
Console#show ip igmp snooping statistics output interface ethernet 1/1
Output Statistics:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Report</th>
<th>Leave</th>
<th>G Query</th>
<th>G(-S)-S Query</th>
<th>Drop</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Table 114: show ip igmp snooping statistics input - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows interface.</td>
</tr>
<tr>
<td>Report</td>
<td>The number of IGMP membership reports received on this interface.</td>
</tr>
<tr>
<td>Leave</td>
<td>The number of leave messages received on this interface.</td>
</tr>
<tr>
<td>G Query</td>
<td>The number of general query messages received on this interface.</td>
</tr>
<tr>
<td>G(-S)-S Query</td>
<td>The number of group specific or group-and-source specific query messages received on this interface.</td>
</tr>
<tr>
<td>Drop</td>
<td>The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.</td>
</tr>
<tr>
<td>Join Succ</td>
<td>The number of times a multicast group was successfully joined.</td>
</tr>
<tr>
<td>Group</td>
<td>The number of multicast groups active on this interface.</td>
</tr>
</tbody>
</table>

Table 115: show ip igmp snooping statistics output - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows interface.</td>
</tr>
<tr>
<td>Report</td>
<td>The number of IGMP membership reports sent from this interface.</td>
</tr>
<tr>
<td>Leave</td>
<td>The number of leave messages sent from this interface.</td>
</tr>
<tr>
<td>G Query</td>
<td>The number of general query messages sent from this interface.</td>
</tr>
<tr>
<td>G(-S)-S Query</td>
<td>The number of group specific or group-and-source specific query messages sent from this interface.</td>
</tr>
<tr>
<td>Drop</td>
<td>The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.</td>
</tr>
<tr>
<td>Group</td>
<td>The number of multicast groups active on this interface.</td>
</tr>
</tbody>
</table>
The following shows IGMP query-related statistics for VLAN 1:

```
Console#show ip igmp snooping statistics query vlan 1
Other Querier             : 192.168.0.1
Other Querier Expire      : 0(m):30(s)
Other Querier Uptime      : 0(h):55(m):0(s)
Self Querier              : 192.168.0.4
Self Querier Expire       : 0(m):0(s)
Self Querier Uptime       : 0(h):0(m):0(s)
General Query Received    : 10
General Query Sent        : 0
Specific Query Received   : 2
Specific Query Sent       : 1
Warn Rate Limit           : 0 sec.
V1 Warning Count          : 0
V2 Warning Count          : 0
V3 Warning Count          : 0
Console#
```

### Table 116: show ip igmp snooping statistics vlan query - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Querier</td>
<td>IP address of remote querier on this interface.</td>
</tr>
<tr>
<td>Other Querier Expire</td>
<td>Time after which remote querier is assumed to have expired.</td>
</tr>
<tr>
<td>Other Querier Uptime</td>
<td>Time remote querier has been up.</td>
</tr>
<tr>
<td>Self Querier</td>
<td>IP address of local querier on this interface.</td>
</tr>
<tr>
<td>Self Querier Expire</td>
<td>Time after which local querier is assumed to have expired.</td>
</tr>
<tr>
<td>Self Querier Uptime</td>
<td>Time local querier has been up.</td>
</tr>
<tr>
<td>General Query Received</td>
<td>The number of general queries received on this interface.</td>
</tr>
<tr>
<td>General Query Sent</td>
<td>The number of general queries sent from this interface.</td>
</tr>
<tr>
<td>Specific Query Received</td>
<td>The number of specific queries received on this interface.</td>
</tr>
<tr>
<td>Specific Query Sent</td>
<td>The number of specific queries sent from this interface.</td>
</tr>
<tr>
<td>Warn Rate Limit</td>
<td>The rate at which received query messages of the wrong version type cause the Vx warning count to increment. Note that “0 sec” means that the Vx warning count is incremented for each wrong message version received.</td>
</tr>
<tr>
<td>V1 Warning Count</td>
<td>The number of times the query version received (Version 1) does not match the version configured for this interface.</td>
</tr>
<tr>
<td>V2 Warning Count</td>
<td>The number of times the query version received (Version 2) does not match the version configured for this interface.</td>
</tr>
<tr>
<td>V3 Warning Count</td>
<td>The number of times the query version received (Version 3) does not match the version configured for this interface.</td>
</tr>
</tbody>
</table>
### Static Multicast Routing

This section describes commands used to configure static multicast routing on the switch.

#### Table 117: Static Multicast Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip igmp snooping vlan mrouter</code></td>
<td>Adds a multicast router port</td>
<td>GC</td>
</tr>
<tr>
<td><code>show ip igmp snooping mrouter</code></td>
<td>Shows multicast router ports</td>
<td>PE</td>
</tr>
</tbody>
</table>

### ip igmp snooping vlan mrouter

This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the `no` form to remove the configuration.

#### Syntax

```
[no] ip igmp snooping vlan vlan-id mrouter interface
```

- `vlan-id`: VLAN ID (Range: 1-4094)
- `interface`: Unit identifier. (Range: 1)
- `port`: Port number. (Range: 1-28/52)
- `port-channel`: Channel-ID (Range: 1-16)

#### Default Setting

No static multicast router ports are configured.

#### Command Mode

Global Configuration

#### Command Usage

- Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.

- IGMP Snooping must be enabled globally on the switch (using the `ip igmp snooping` command) before a multicast router port can take effect.
Example
The following shows how to configure port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

IGMP Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 118: IGMP Filtering and Throttling Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp filter</td>
<td>Enables IGMP filtering and throttling on the switch</td>
<td>GC</td>
</tr>
<tr>
<td>ip igmp profile</td>
<td>Sets a profile number and enters IGMP filter profile</td>
<td>GC</td>
</tr>
<tr>
<td>permit, deny</td>
<td>Sets a profile access mode to permit or deny</td>
<td>IPC</td>
</tr>
<tr>
<td>range</td>
<td>Specifies one or a range of multicast addresses for a</td>
<td>IPC</td>
</tr>
<tr>
<td></td>
<td>profile</td>
<td></td>
</tr>
<tr>
<td>ip igmp authentication</td>
<td>Enables RADIUS authentication for IGMP JOIN requests.</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp filter</td>
<td>Assigns an IGMP filter profile to an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp max-groups</td>
<td>Specifies an IGMP throttling number for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp max-groups action</td>
<td>Sets the IGMP throttling action for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ip igmp query-drop</td>
<td>Drops any received IGMP query packets</td>
<td>IC</td>
</tr>
<tr>
<td>ip multicast-data-drop</td>
<td>Drops all multicast data packets</td>
<td>IC</td>
</tr>
<tr>
<td>show ip igmp authentication</td>
<td>Displays IGMP authentication settings for interfaces</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp filter</td>
<td>Displays the IGMP filtering status</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp profile</td>
<td>Displays IGMP profiles and settings</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp query-drop</td>
<td>Shows if the interface is configured to drop IGMP query</td>
<td>PE</td>
</tr>
<tr>
<td></td>
<td>packets</td>
<td></td>
</tr>
<tr>
<td>show ip igmp throttle</td>
<td>Displays the IGMP throttling setting for interfaces</td>
<td>PE</td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td></td>
</tr>
<tr>
<td>show ip multicast-data-</td>
<td>Shows if the interface is configured to drop multicast</td>
<td>PE</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td></td>
</tr>
</tbody>
</table>
**ip igmp filter**  
*(Global Configuration)*  
This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

**Syntax**

```plaintext
[no] ip igmp filter
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

- The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

**Example**

```
Console(config)#ip igmp filter
Console(config)#
```

**ip igmp profile**  
This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

**Syntax**

```plaintext
[no] ip igmp profile profile-number
```

`profile-number` - An IGMP filter profile number. (Range: 1-4294967295)

**Default Setting**

Disabled

**Command Mode**

Global Configuration
Command Usage
A profile defines the multicast groups that a subscriber is permitted or denied to
join. The same profile can be applied to many interfaces, but only one profile can
be assigned to one interface. Each profile has only one access mode; either permit
or deny.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

**permit, deny** This command sets the access mode for an IGMP filter profile. Use the no form to
delete a profile number.

**Syntax**

```
(permit | deny)
```

**Default Setting**
Deny

**Command Mode**
IGMP Profile Configuration

**Command Usage**

◆ Each profile has only one access mode; either permit or deny.

◆ When the access mode is set to permit, IGMP join reports are processed when a
multicast group falls within the controlled range. When the access mode is set
to deny, IGMP join reports are only processed when a multicast group is not in
the controlled range.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

**range** This command specifies multicast group addresses for a profile. Use the no form to
delete addresses from a profile.

**Syntax**

```
[no] range low-ip-address [high-ip-address]
```

low-ip-address - A valid IP address of a multicast group or start of a group
range.

high-ip-address - A valid IP address for the end of a multicast group range.
Default Setting
None

Command Mode
IGMP Profile Configuration

Command Usage
Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1 239.2.3.100
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

**ip igmp authentication**  This command enables IGMP authentication on the specified interface. When enabled and an IGMP JOIN request is received, an authentication request is sent to a configured RADIUS server. Use the **no** form to disable IGMP authentication.

Syntax

```
[no] ip igmp authentication
```

Default Setting
Disabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage

- If IGMP authentication is enabled on an interface, and a join report is received on the interface, the switch will send an access request to the RADIUS server to perform authentication.

- Only when the RADIUS server responds with an authentication success message will the switch learn the group report. Once the group is learned, the switch will not send an access request to the RADIUS server when receiving the same report again within a one (1) day period.

- If the RADIUS server responds that authentication failed or the timer expires, the report will be dropped and the group will not be learned. The entry (host MAC, port number, VLAN ID, and group IP) will be put in the “authentication failed list”.

- The “authentication failed list” is valid for the period of the interval defined by the command **ip igmp snooping vlan query-interval**. When receiving the same
report during this interval, the switch will not send the access request to the RADIUS server.

- If the interface leaves the group and subsequently rejoins the same group, the join report needs to again be authenticated.

- When receiving an IGMP v3 report message, the switch will send the access request to the RADIUS server only when the record type is either IS_EX or TO_EX, and the source list is empty. Other types of packets will not initiate RADIUS authentication.

  **IS_EX (MODE_IS_EXCLUDE)** - Indicates that the interface's filter mode is EXCLUDE for the specified multicast address. The Source Address fields in this Group Record contain the interface's source list for the specified multicast address, if not empty.

  **TO_EX (CHANGE_TO_EXCLUDE_MODE)** - Indicates that the interface has changed to EXCLUDE filter mode for the specified multicast address. The Source Address fields in this Group Record contain the interface's new source list for the specified multicast address, if not empty.

- When a report is received for the first time and is being authenticated, whether authentication succeeds or fails, the report will still be sent to the multicast-router port.

- The following table shows the RADIUS server Attribute Value Pairs used for authentication:

  **Table 119: IGMP Authentication RADIUS Attribute Value Pairs**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Type</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_NAME</td>
<td>1</td>
<td>User MAC address</td>
</tr>
<tr>
<td>USER_PASSWORD</td>
<td>2</td>
<td>User MAC address</td>
</tr>
<tr>
<td>NAS_IP_ADDRESS</td>
<td>4</td>
<td>Switch IP address</td>
</tr>
<tr>
<td>NAS_PORT</td>
<td>5</td>
<td>User Port Number</td>
</tr>
<tr>
<td>FRAMED_IP_ADDRESS</td>
<td>8</td>
<td>Multicast Group ID</td>
</tr>
</tbody>
</table>

  **Example**

  This example shows how to enable IGMP Authentication on all of the switch’s Ethernet interfaces.

  ```
  Console(config)#interface ethernet 1/1-28
  Console(config-if)#ip igmp authentication
  Console#
  ```

  **Related Commands**

  `show ip igmp authentication`
**ip igmp filter**  
* (Interface Configuration)  
This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

**Syntax**

```
[no] ip igmp filter profile-number
```

*profile-number* - An IGMP filter profile number. (Range: 1-4294967295)

**Default Setting**

None

**Command Mode**

Interface Configuration

**Command Usage**

◆ The IGMP filtering profile must first be created with the **ip igmp profile** command before being able to assign it to an interface.

◆ Only one profile can be assigned to an interface.

◆ A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

**ip igmp max-groups**  
This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

**Syntax**

```
ip igmp max-groups number

no ip igmp max-groups
```

*number* - The maximum number of multicast groups an interface can join at the same time. (Range: 1-1023)

**Default Setting**

1023

**Command Mode**

Interface Configuration (Ethernet, Port Channel)
Chapter 21 | Multicast Filtering Commands
IGMP Filtering and Throttling

Command Usage
◆ IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

◆ IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example
```console
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

**ip igmp max-groups**

This command sets the IGMP throttling action for an interface on the switch.

**Syntax**
```
ip igmp max-groups action {deny | replace}
```

**deny** - The new multicast group join report is dropped.

**replace** - The new multicast group replaces an existing group.

**Default Setting**
Deny

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

**Example**
```console
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```
**ip igmp query-drop**  This command drops any received IGMP query packets. Use the no form to restore the default setting.

**Syntax**

```plaintext
[no] ip igmp query-drop
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

---

**ip multicast-data-drop**  This command drops all multicast data packets. Use the **no** form to disable this feature.

**Syntax**

```plaintext
[no] ip multicast-data-drop
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

This command can be used to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```
**show ip igmp authentication**

This command displays the interface settings for IGMP authentication.

**Syntax**

```
show ip igmp authentication interface [interface]
```

- `interface`
  - `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Command Usage**

Using this command without specifying an interface displays information for all interfaces.

**Example**

```
Console#show ip igmp authentication
Ethernet 1/1: Enabled
Ethernet 1/2: Enabled
Ethernet 1/3: Enabled
...
Ethernet 1/27: Enabled
Ethernet 1/28: Enabled
Other ports/port channels are Disable
Console#
```

**show ip igmp filter**

This command displays the global and interface settings for IGMP filtering.

**Syntax**

```
show ip igmp filter [interface interface]
```

- `interface`
  - `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)

**Default Setting**

None
**Command Mode**
Privileged Exec

**Example**

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
---------------------------------
IGMP Profile 19
Deny
 Range 239.1.1.1 239.1.1.1
 Range 239.2.3.1 239.2.3.100
Console#
```

**show ip igmp profile**
This command displays IGMP filtering profiles created on the switch.

**Syntax**

```
show ip igmp profile [profile-number]
```

*profile-number* - An existing IGMP filter profile number.
(Range: 1-4294967295)

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
 Deny
 Range 239.1.1.1 239.1.1.1
 Range 239.2.3.1 239.2.3.100
Console#
```
show ip igmp query-drop

This command shows if the specified interface is configured to drop IGMP query packets.

Syntax

```
show ip igmp throttle interface [interface]
```

```
interface
  ethernet unit/port
    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)
  port-channel channel-id (Range: 1-16)
```

Default Setting
None

Command Mode
Privileged Exec

Command Usage
Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

Syntax

```
show ip igmp throttle interface [interface]
```

```
interface
  ethernet unit/port
    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)
  port-channel channel-id (Range: 1-16)
```

Default Setting
None

Command Mode
Privileged Exec
**Command Usage**

Using this command without specifying an interface displays information for all interfaces.

**Example**

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
    Status : FALSE
    Action : Deny
    Max Multicast Groups : 1023
    Current Multicast Groups : 0

Console#
```

**show ip multicast-data-drop**

This command shows if the specified interface is configured to drop multicast data packets.

**Syntax**

```
show ip igmp throttle interface [interface]
```

interface

- **ethernet unit/port**
  - **unit** - Unit identifier. (Range: 1)
  - **port** - Port number. (Range: 1-28/52)
- **port-channel channel-id** (Range: 1-16)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Command Usage**

Using this command without specifying an interface displays all interfaces.

**Example**

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```
MLD Snooping

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Table 120: MLD Snooping Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping</td>
<td>Enables MLD Snooping globally</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping querier</td>
<td>Allows the switch to act as the querier for MLD snooping</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping query-interval</td>
<td>Configures the interval between sending MLD general</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>query messages</td>
<td></td>
</tr>
<tr>
<td>ipv6 mld snooping query-max-response-time</td>
<td>Configures the maximum response time for a general</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>queries</td>
<td></td>
</tr>
<tr>
<td>ipv6 mld snooping proxy-reporting</td>
<td>Enables MLD Snooping with Proxy Reporting</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping robustness</td>
<td>Configures the robustness variable</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping router-port-expire-time</td>
<td>Configures the router port expire time</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping unknown-multicast mode</td>
<td>Sets an action for unknown multicast packets</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping unsolicited-report-interval</td>
<td>Specifies how often the upstream interface should</td>
<td>GC</td>
</tr>
<tr>
<td></td>
<td>transmit unsolicited IGMP reports (when proxy reporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is enabled)</td>
<td></td>
</tr>
<tr>
<td>ipv6 mld snooping version</td>
<td>Configures the MLD Snooping version</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping vlan</td>
<td>Removes a member port of an IPv6 multicast service if a</td>
<td>GC</td>
</tr>
<tr>
<td>immediate-leave</td>
<td>leave packet is received at that port and MLD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>immediate-leave is enabled for the parent VLAN</td>
<td></td>
</tr>
<tr>
<td>ipv6 mld snooping vlan mrouter</td>
<td>Adds an IPv6 multicast router port</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld snooping vlan static</td>
<td>Adds an interface as a member of a multicast group</td>
<td>GC</td>
</tr>
<tr>
<td>clear ipv6 mld snooping groups</td>
<td>Clears multicast group information dynamically learned</td>
<td>PE</td>
</tr>
<tr>
<td>groups dynamic</td>
<td>through MLD snooping</td>
<td></td>
</tr>
</tbody>
</table>
ipv6 mld snooping

This command enables MLD Snooping globally on the switch. Use the `no` form to disable MLD Snooping.

**Syntax**

```
[no] ipv6 mld snooping
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Example**
The following example enables MLD Snooping:

```
Console(config)#ipv6 mld snooping
```

ipv6 mld snooping querier

This command allows the switch to act as the querier for MLDv2 snooping. Use the no form to disable this feature.

**Syntax**

```
[no] ipv6 mld snooping querier
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

---

### Table 120: MLD Snooping Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 mld snooping statistics</td>
<td>Clears MLD snooping statistics</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld snooping</td>
<td>Displays MLD Snooping configuration</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld snooping group</td>
<td>Displays the learned groups</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld snooping group source-list</td>
<td>Displays the learned groups and corresponding source list</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld snooping mrouter</td>
<td>Displays the information of multicast router ports</td>
<td>PE</td>
</tr>
<tr>
<td>show ip igmp snooping statistics</td>
<td>Shows IGMP snooping protocol statistics for the specified interface</td>
<td>PE</td>
</tr>
</tbody>
</table>
**MLD Snooping**

**Command Usage**

◆ If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

◆ An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses its own IPv6 address as the query source address.

◆ The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

**Example**

```
Console(config)#ipv6 mld snooping querier
Console(config)#
```

**ipv6 mld snooping query-interval**

This command configures the interval between sending MLD general queries. Use the **no** form to restore the default.

**Syntax**

```
ipv6 mld snooping query-interval interval
no ipv6 mld snooping query-interval
```

*interval* - The interval between sending MLD general queries.

(Range: 60-125 seconds)

**Default Setting**

125 seconds

**Command Mode**

Global Configuration

**Command Usage**

◆ This command applies when the switch is serving as the querier.

◆ An MLD general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

**Example**

```
Console(config)#ipv6 mld snooping query-interval 125
Console(config)#
```
**ipv6 mld snooping query-max-response-time**

This command configures the maximum response time advertised in MLD general queries. Use the `no` form to restore the default.

**Syntax**

```
ipv6 mld snooping query-max-response-time seconds
no ipv6 mld snooping query-max-response-time
```

- `seconds` - The maximum response time allowed for MLD general queries.
  (Range: 5-25 seconds)

**Default Setting**

10 seconds

**Command Mode**

Global Configuration

**Command Usage**

This command controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

**Example**

```
Console(config)#ipv6 mld snooping query-max-response-time seconds 15
Console(config)#
```

**ipv6 mld snooping proxy-reporting**

This command enables IGMP Snooping with Proxy Reporting. Use the `no` form to restore the default setting.

**Syntax**

```
[no] ipv6 mld snooping proxy-reporting
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- When proxy reporting is enabled with this command, reports received from downstream hosts are summarized and used to build internal membership states. Proxy-reporting devices may use the all-zeros IP source address when forwarding any summarized reports upstream. For this reason, IGMP membership reports received by the snooping switch must not be rejected because the source IP address is set to 0.0.0.0.
ipv6 mld snooping robustness  This command configures the MLD Snooping robustness variable. Use the no form to restore the default value.

**Syntax**

```
ipv6 mld snooping robustness value
no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)
```

**Default Setting**

2

**Command Mode**

Global Configuration

**Command Usage**

A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

**Example**

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port-expire-time  This command configures the MLD query timeout. Use the no form to restore the default.

**Syntax**

```
ipv6 mld snooping router-port-expire-time time
no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port. (Range: 300-500 seconds)
```

**Default Setting**

300 seconds

**Command Mode**

Global Configuration
Chapter 21 | Multicast Filtering Commands
MLD Snooping

**Command Usage**
The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

**Example**

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

**ipv6 mld snooping unknown-multicast mode**
This command sets the action for dealing with unknown multicast packets. Use the `no` form to restore the default.

**Syntax**

```
ipv6 mld snooping unknown-multicast mode {flood | to-router-port}
no ipv6 mld snooping unknown-multicast mode
```

- **flood** - Floods the unknown multicast data packets to all ports.
- **to-router-port** - Forwards the unknown multicast data packets to router ports.

**Default Setting**
to-router-port

**Command Mode**
Global Configuration

**Command Usage**
- When set to “flood,” any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.
- When set to “router-port,” any received IPv6 multicast packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

**Example**

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

**ipv6 mld snooping unsolicited-report-interval**
This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the `no` form to restore the default value.
MLD Snooping

Syntax

ipv6 mld snooping unsolicited-report-interval seconds

no ipv6 mld snooping unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports.
(Range: 1-65535 seconds)

Default Setting
400 seconds

Command Mode
Global Configuration

Command Usage
◆ When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.

◆ This command only applies when proxy reporting is enabled (see page 611).

Example

Console(config)#ipv6 mld snooping unsolicited-report-interval 5
Console(config)#

ipv6 mld snooping version

This command configures the MLD snooping version. Use the no form to restore the default.

Syntax

ipv6 mld snooping version {1 | 2}

1 - MLD version 1.
2 - MLD version 2.

Default Setting
Version 2

Command Mode
Global Configuration

Example

Console(config)#ipv6 mld snooping version 1
Console(config)#
**ipv6 mld snooping vlan immediate-leave**

This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the `no` form to restore the default.

**Syntax**

```
[no] ipv6 mld snooping vlan vlan-id immediate-leave
```

- `vlan-id`: A VLAN identification number. (Range: 1-4094)

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- If MLD immediate-leave is not used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

- If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

**Example**

The following shows how to enable MLD immediate leave.

```
Console(config)#ipv6 mld snooping immediate-leave
Console(config-if)#
```

**ipv6 mld snooping vlan mrouter**

This command statically configures an IPv6 multicast router port. Use the `no` form to remove the configuration.

**Syntax**

```
[no] ipv6 mld snooping vlan vlan-id mrouter interface
```

- `vlan-id`: VLAN ID (Range: 1-4094)
- `interface`:
  - `ethernet unit/port`
    - `unit`: Unit identifier. (Range: 1)
    - `port`: Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)
Default Setting
No static multicast router ports are configured.

Command Mode
Global Configuration

Command Usage
Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Example
The following shows how to configure port 1 as a multicast router port within VLAN 1:

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

```
ipv6 mld snooping
```

This command adds a port to an IPv6 multicast group. Use the no form to remove the port.

Syntax

```
[no] ipv6 mld snooping vlan vlan-id static ipv6-address interface

vlan - VLAN ID (Range: 1-4094)
ipv6-address - An IPv6 address of a multicast group. (Format: X::X::X)
interface

ethernet unit/port

unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)
```

Default Setting
None

Command Mode
Global Configuration

Example

```
Console(config)#ipv6 mld snooping vlan 1 static ff05:0:1:2:3:4:5:6 ethernet 1/6
Console(config)#
```
clear ipv6 mld snooping groups dynamic

This command clears multicast group information dynamically learned through MLD snooping.

Syntax

   clear ipv6 mld snooping groups dynamic

Command Mode
Privileged Exec

Command Usage
This command only clears entries learned though MLD snooping. Statically configured multicast address are not cleared.

Example

```
Console#clear ipv6 mld snooping groups dynamic
Console#
```

clear ipv6 mld snooping statistics

This command clears MLD snooping statistics.

Syntax

   clear ipv6 mld snooping statistics [interface interface]  
      interface
         ethernet unit/port
            unit - Unit identifier. (Range: 1)
            port - Port number. (Range: 1-28/52)
      port-channel channel-id (Range: 1-16)
      vlan vlan-id - VLAN identifier (Range: 1-4094)

Command Mode
Privileged Exec

Example

```
Console#clear ipv6 mld snooping statistics
Console#
```
**show ipv6 mld snooping**

This command shows the current MLD Snooping configuration.

**Syntax**

```
show ipv6 mld snooping [vlan vlan-id]
```

- **vlan-id** - VLAN ID (1-4094)

**Command Mode**

Privileged Exec

**Command Usage**

This command displays global and VLAN-specific MLD snooping configuration settings.

**Example**

The following shows MLD Snooping configuration information

```
Console#show ipv6 mld snooping
Service Status : Disabled
Proxy Reporting : Disabled
Querier Status : Disabled
Robustness : 2
Query Interval : 125 sec
Query Max Response Time : 10 sec
Router Port Expiry Time : 300 sec
Unsolicit Report Interval : 400 sec
Immediate Leave : Disabled on all VLAN
Immediate Leave By Host : Disabled on all VLAN
Unknown Flood Behavior : To Router Port
MLD Snooping Version : Version 2

VLAN Group IPv6 Address Port
---- --------------------------------------- ---------
1 ff05:0:1:2:3:4:5:6 Eth 1/1

Console#
```

**show ipv6 mld snooping group**

This command shows known multicast groups, member ports, and the means by which each group was learned.

**Syntax**

```
show ipv6 mld snooping group
```

**Command Mode**

Privileged Exec
Example
The following shows MLD Snooping group configuration information:

```
Table: MLD Snooping Group Configuration

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Multicast IPv6 Address</th>
<th>Member Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FF02::01:01:01:01</td>
<td>Eth 1/1</td>
<td>MLD Snooping</td>
</tr>
<tr>
<td>1</td>
<td>FF02::01:01:01:02</td>
<td>Eth 1/1</td>
<td>Multicast Data</td>
</tr>
<tr>
<td>1</td>
<td>FF02::01:01:01:02</td>
<td>Eth 1/1</td>
<td>User</td>
</tr>
</tbody>
</table>
```

```
show ipv6 mld snooping group

This command shows known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

Syntax
```
show ipv6 mld snooping group source-list
```

Command Mode
Privileged Exec

Example
The following shows MLD Snooping group mapping information:

```
Table: MLD Snooping Group Mapping

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Multicast IPv6 Address</th>
<th>Member Port</th>
<th>Type</th>
<th>Filter Mode</th>
<th>Filter Timer elapse</th>
<th>Request List</th>
<th>Exclude List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FF02::01:01:01:01</td>
<td>Eth 1/1</td>
<td>MLD Snooping</td>
<td>Include</td>
<td>10 sec.</td>
<td>::01:02:03:04, ::01:02:03:05, ::01:02:03:06, ::01:02:03:07</td>
<td>::02:02:03:04, ::02:02:03:05, ::02:02:03:06, ::02:02:03:07</td>
</tr>
<tr>
<td>1</td>
<td>FF02::01:01:01:02</td>
<td>Eth 1/1</td>
<td>Multicast Data</td>
<td>Include</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>FF02::01:01:01:02</td>
<td>Eth 1/1</td>
<td>User</td>
<td>Exclude</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Option:
Filter Mode: Include, Exclude
```

Console#
Chapter 21 | Multicast Filtering Commands
MLD Snooping

show ipv6 mld snooping mrouter
This command shows MLD Snooping multicast router information.

Syntax

```
show ipv6 mld snooping mrouter vlan vlan-id
```

- `vlan-id` - A VLAN identification number. (Range: 1-4094)

Command Mode
Privileged Exec

Example

```
Console#show ipv6 mld snooping mrouter vlan 1
VLAN Multicast Router Port Type      Expire
---- --------------------- --------- ------
1 Eth 1/ 2              Static

Console#
```

show ipv6 mld snooping statistics
This command shows MLD snooping protocol statistics for the specified interface.

Syntax

```
show ipv6 mld snooping statistics
```

- `interface`
  - `ethernet unit/port`
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)
  - `vlan vlan-id` - VLAN ID (Range: 1-4094)
- `query` - Displays IGMP snooping-related statistics.

Default Setting
None

Command Mode
Privileged Exec
Example
The following shows MLD protocol statistics input:

```
Console# show ipv6 mld snooping statistics input interface ethernet 1/1
Input Statistics:
            Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
            --------- -------- -------- -------- ------------- -------- --------- ------
        Eth 1/ 1        23       11        4            10        5        14      5
Console#
```

MLD Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

Table 121: MLD Filtering and Throttling Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld filter</td>
<td>Enables MLD filtering and throttling on the switch</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 mld profile</td>
<td>Sets a profile number and enters MLD filter profile configuration mode</td>
<td>GC</td>
</tr>
<tr>
<td>permit, deny</td>
<td>Sets a profile access mode to permit or deny</td>
<td>IPC</td>
</tr>
<tr>
<td>range</td>
<td>Specifies one or a range of multicast addresses for a profile</td>
<td>IPC</td>
</tr>
<tr>
<td>ipv6 mld filter</td>
<td>Assigns an MLD filter profile to an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 mld max-groups</td>
<td>Specifies an M:D throttling number for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 mld max-groups action</td>
<td>Sets the MLD throttling action for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 mld query-drop</td>
<td>Drops any received MLD query packets</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 multicast-data-drop</td>
<td>Enable multicast data drop mode on a port interface</td>
<td>IC</td>
</tr>
<tr>
<td>show ipv6 mld filter</td>
<td>Displays the MLD filtering status</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld profile</td>
<td>Displays MLD profiles and settings</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld query-drop</td>
<td>Shows if the interface is configured to drop MLD query packets</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mld throttle interface</td>
<td>Displays the MLD throttling setting for interfaces</td>
<td>PE</td>
</tr>
</tbody>
</table>
**ipv6 mld filter**

*(Global Configuration)*

This command globally enables MLD filtering and throttling on the switch. Use the **no** form to disable the feature.

**Syntax**

```
[no] ipv6 mld filter
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

◆ MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

◆ MLD filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

◆ The MLD filtering feature operates in the same manner when MVR6 is used to forward multicast traffic.

**Example**

```
Console(config)#ipv6 mld filter
Console(config)#
```

**Related Commands**

* show ipv6 mld filter

---

**ipv6 mld profile**

This command creates an MLD filter profile number and enters MLD profile configuration mode. Use the **no** form to delete a profile number.

**Syntax**

```
[no] ipv6 mld profile profile-number
```

*profile-number* - An MLD filter profile number. (Range: 1-4294967295)

**Default Setting**

Disabled
Command Mode
Global Configuration

Command Usage
A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#
```

Related Commands
show ipv6 mld profile

**permit, deny**

This command sets the access mode for an MLD filter profile. Use the `no` form to delete a profile number.

Syntax

```
{permit | deny}
```

Default Setting
deny

Command Mode
MLD Profile Configuration

Command Usage

◆ Each profile has only one access mode; either permit or deny.

◆ When the access mode is set to permit, MLD join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, MLD join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#permit
Console(config-mld-profile)#
```

**range**

This command specifies multicast group addresses for a profile. Use the `no` form to delete addresses from a profile.
Syntax

```plaintext
[no] range low-ipv6-address [high-ipv6-address]
```

- **low-ipv6-address**: A valid IPv6 address (X:X:X::X) of a multicast group or start of a group range.
- **high-ipv6-address**: A valid IPv6 address (X:X:X::X) for the end of a multicast group range.

**Default Setting**
None

**Command Mode**
MLD Profile Configuration

**Command Usage**
Enter this command multiple times to specify more than one multicast address or address range for a profile.

**Example**
```
Console(config-mld-profile)#range ff01::0101 ff01::0202
```

---

**ipv6 mld filter**
(Interface Configuration)

This command assigns an MLD filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

**Syntax**

```plaintext
[no] ipv6 mld filter profile-number
```

- **profile-number**: An MLD filter profile number. (Range: 1-4294967295)

**Default Setting**
None

**Command Mode**
Interface Configuration

**Command Usage**

- The MLD filtering profile must first be created with the `ipv6 mld profile` command before being able to assign it to an interface.

- Only one profile can be assigned to an interface.

- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.
**ipv6 mld max-groups**

This command configures the maximum number of MLD groups that an interface can join. Use the `no` form to restore the default setting.

**Syntax**

```
ipv6 mld max-groups number

no ipv6 mld max-groups
```

- `number` - The maximum number of multicast groups an interface can join at the same time. (Range: 1-255)

**Default Setting**

255

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

- MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

- MLD throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

- If the maximum number of MLD groups is set to the default value, the running status of MLD throttling will change to false. This means that any configuration for MLD throttling will have no effect until the maximum number of MLD groups is configured to another value.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld filter 19
Console(config-if)#
```

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups 10
Console(config-if)#
```
**ipv6 mld max-groups action**  This command sets the MLD throttling action for an interface on the switch.

**Syntax**

```
ipv6 mld max-groups action {deny | replace}

deny - The new multicast group join report is dropped.
replace - The new multicast group replaces an existing group.
```

**Default Setting**
Deny

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups action replace
Console(config-if)#
```

**ipv6 mld query-drop**  This command drops any received MLD query packets. Use the no form to restore the default setting.

**Syntax**

```
[no] ipv6 mld query-drop
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.
### ipv6 multicast-data-drop

Use this command to enable multicast data drop mode on a port interface. Use the `no` form of the command to disable multicast data drop.

**Syntax**

```
[no] ipv6 multicast-data-drop
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Example**

```bash
Console(config)#interface ethernet 1/3
Console(config-if)#ipv6 multicast-data-drop
Console(config-if)#
```

### show ipv6 mld filter

This command displays the global and interface settings for MLD filtering.

**Syntax**

```
show ipv6 mld filter [interface interface]
```

- `interface`:
  - `ethernet unit/port`
    - `unit` - Unit identifier. (Range: 1)
    - `port` - Port number. (Range: 1-28/52)
  - `port-channel channel-id` (Range: 1-16)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```bash
Console#show ipv6 mld filter
MLD filter Enabled
Console#show ipv6 mld filter interface ethernet 1/3
```
Chapter 21 | Multicast Filtering Commands
MLD Filtering and Throttling

show ipv6 mld profile

This command displays MLD filtering profiles created on the switch.

**Syntax**

```plaintext
show ipv6 mld profile [profile-number]
```

*profile-number* - An existing MLD filter profile number.
(Range: 1-4294967295)

**Default Setting**
None

**Command Mode**
Privileged Exec

**Example**

```
Console#show ipv6 mld profile
MLD Profile 19
MLD Profile 50
Console#show ipv6 mld profile 19
MLD Profile 19
Deny
Range ff01::101 ff01::faa
Console#show ipv6 mld profile 5
MLD Profile 19
Deny
Range ff01::101 ff01::faa
Console#
```

show ipv6 mld query-drop

This command shows if the specified interface is configured to drop MLD query packets.

**Syntax**

```plaintext
show ipv6 mld query-drop interface [interface]
```

*interface*

```plaintext
ethernet unit/port
```

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-28/52)

*port-channel channel-id* (Range: 1-16)
Default Setting
None

Command Mode
Privileged Exec

Command Usage
Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ipv6 mld query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

```
show ipv6 mld throttle interface
```
This command displays the interface settings for MLD throttling.

Syntax
```
show ipv6 mld throttle interface [interface]
```

```
interface
```
```
ethernet unit/port
```

```
unit - Unit identifier. (Range: 1)
```

```
port - Port number. (Range: 1-28/52)
```

```
port-channel channel-id (Range: 1-16)
```

Default Setting
None

Command Mode
Privileged Exec

Command Usage
Using this command without specifying an interface displays information for all interfaces.

Example

```
Console#show ipv6 mld throttle interface ethernet 1/3
Eth  1/3 Information
    Status : TRUE
    Action : Replace
    Max Multicast Groups : 10
    Current Multicast Groups : 0

Console#
```
Multicast VLAN Registration for IPv4

This section describes commands used to configure Multicast VLAN Registration for IPv4 (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider’s network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 122: Multicast VLAN Registration for IPv4 Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mvr</td>
<td>Globally enables MVR</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr associated-profile</td>
<td>Binds the MVR group addresses specified in a profile to an MVR domain</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr domain</td>
<td>Enables MVR for a specific domain</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr group</td>
<td>Statically configures MVR group address(es)</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr priority</td>
<td>Assigns a priority to all multicast traffic in the MVR VLAN</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr profile</td>
<td>Maps a range of MVR group addresses to a profile</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr proxy-query-interval</td>
<td>Configures the interval at which the receiver port sends out general queries.</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr proxy-switching</td>
<td>Enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr robustness-value</td>
<td>Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr source-port-mode</td>
<td>Configures the switch to only forward multicast streams which the source port has dynamically joined</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>dynamic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mvr upstream-source-ip</td>
<td>Configures the source IP address assigned to all control packets sent upstream</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr vlan</td>
<td>Specifies the VLAN through which MVR multicast data is received</td>
<td></td>
<td>GC</td>
</tr>
<tr>
<td>mvr immediate-leave</td>
<td>Enables immediate leave capability</td>
<td></td>
<td>IC</td>
</tr>
<tr>
<td>mvr type</td>
<td>Configures an interface as an MVR receiver or source port</td>
<td></td>
<td>IC</td>
</tr>
<tr>
<td>mvr vlan group</td>
<td>Statically binds a multicast group to a port</td>
<td></td>
<td>IC</td>
</tr>
<tr>
<td>clear mvr groups dynamic</td>
<td>Clears multicast group information dynamically learned through MVR</td>
<td></td>
<td>PE</td>
</tr>
<tr>
<td>clear mvr statistics</td>
<td>Clears MVR statistics</td>
<td></td>
<td>PE</td>
</tr>
<tr>
<td>show mvr</td>
<td>Shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address</td>
<td></td>
<td>PE</td>
</tr>
</tbody>
</table>
**mvr**  This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the **no** form of this command to globally disable MVR.

**Syntax**

```text
[no] mvr
```

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the `mvr vlan group` command.

**Example**

The following example enables MVR globally.

```text
Console(config)#mvr
```

**mvr associated-profile**  This command binds the MVR group addresses specified in a profile to an MVR domain. Use the **no** form of this command to remove the binding.

**Syntax**

```text
[no] mvr domain domain-id associated-profile profile-name
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
- `profile-name` - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Example**
The following an MVR group address profile to domain 1:

```
Console(config)#mvr domain 1 associated-profile rd
Console(config)#
```

**Related Commands**
`mvr profile (634)`

### mvr domain

This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the `no` form of this command to disable MVR for a domain.

**Syntax**

```
[no] mvr domain domain-id
```

`domain-id` - An independent multicast domain. (Range: 1-5)

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the `mvr vlan group` command.

**EXAMPLE**
The following example enables MVR for domain 1:

```
Console(config)#mvr domain 1
Console(config)#
```
mvr group

This command statically configures MVR multicast group IP address(es).

Syntax

```
mvr group {start-ip-address [end-ip-address] | start-ip-address count}
```

- **ip-address** - IP address or address range for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- **count** - The number of contiguous MVR group addresses. (Range: 1-255)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Use the mvr group command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

- This command is obsolete and has been retained only for backward compatibility with earlier software releases. When used, it creates an mvr profile and mvr domain entry in the running-config. The no form of this command has therefore been replaced by the no form of the mvr profile and mvr domain commands.

Example

```
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

mvr priority

This command assigns a priority to all multicast traffic in the MVR VLAN. Use the no form of this command to restore the default setting.

Syntax

```
mvr priority priority

no mvr priority
```

- **priority** - The CoS priority assigned to all multicast traffic forwarded into the MVR VLAN. (Range: 0-7, where 7 is the highest priority)
Chapter 21 | Multicast Filtering Commands
Multicast VLAN Registration for IPv4

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

**Example**

```
Console(config)#mvr priority 6
Console(config)#
```

**Related Commands**
*show mvr*

**mvr profile**
This command maps a range of MVR group addresses to a profile. Use the no form of this command to remove the profile.

**Syntax**

```
mvr profile profile-name start-ip-address end-ip-address
no mvr profile profile-name
```

- **profile-name** - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- **start-ip-address** - Starting IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- **end-ip-address** - Ending IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

**Default Setting**
No profiles are defined

**Command Mode**
Global Configuration

**Command Usage**
- Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

IGMP snooping and MVR share a maximum number of 1023 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

**Example**
The following example maps a range of MVR group addresses to a profile:

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```

**mvr proxy-query-interval**
This command configures the interval at which the receiver port sends out general queries. Use the no form to restore the default setting.

**Syntax**

```
mvr proxy-query-interval interval
no mvr proxy-query-interval
```

- interval - The interval at which the receiver port sends out general queries.
  (Range: 2-31744 seconds)

**Default Setting**
125 seconds

**Command Mode**
Global Configuration

**Command Usage**
This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the mvr proxy-switching command.

**Example**
This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr proxy-query-interval 250
Console(config)#
```
**mvr proxy-switching**  This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the `no` form to disable this function.

**Syntax**

```plaintext
[no] mvr proxy-switching
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Command Usage**

- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.

- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.

- When the source port receives report and leave messages, it only forwards them to other source ports.

- When receiver ports receive any query messages, they are dropped.

- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.

- When MVR proxy switching is disabled:
  - Any membership reports received from receiver/source ports are forwarded to all source ports.
  - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
  - When a receiver port receives a query message, it will be dropped.

**Example**

The following example enable MVR proxy switching.

```
Console(config)#mvr proxy-switching
Console(config)#
```
Related Commands

**mvr robustness-value (637)**

**mvr robustness-value**

This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the no form to restore the default setting.

**Syntax**

```
  mvr robustness-value value
  no mvr robustness-value
```

- `value` - The robustness used for all interfaces. (Range: 1-255)

**Default Setting**

2

**Command Mode**

Global Configuration

**Command Usage**

- This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.

- This command only takes effect when MVR proxy switching is enabled.

**Example**

```
Console(config)#mvr robustness-value 5
Console(config)#
```

**Related Commands**

**mvr proxy-switching (636)**

**mvr source-port-mode**

This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the no form to restore the default setting.

**Syntax**

```
  [no] mvr source-port-mode dynamic
```

**Default Setting**

Forwards all multicast streams which have been specified in a profile and bound to a domain.

**Command Mode**

Global Configuration
Command Usage

◆ By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

◆ When the `mvr source-port-mode dynamic` command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Example

```
Console(config)#mvr source-port-mode dynamic
Console(config)#
```

`mvr upstream-source-ip` This command configures the source IP address assigned to all MVR control packets sent upstream on all domains or on a specified domain. Use the `no` form to restore the default setting.

Syntax

```
mvr [domain domain-id] upstream-source-ip source-ip-address
no mvr [domain domain-id] upstream-source-ip
```

`domain-id` - An independent multicast domain. (Range: 1-5)

`source-ip-address` – The source IPv4 address assigned to all MVR control packets sent upstream.

Default Setting
All MVR reports sent upstream use a null source IP address

Command Mode
Global Configuration

Example

```
Console(config)#mvr domain 1 upstream-source-ip 192.168.0.3
Console(config)#
```
mvr vlan  This command specifies the VLAN through which MVR multicast data is received. Use the no form of this command to restore the default MVR VLAN.

Syntax

```
mvr [domain domain-id] vlan vlan-id
no mvr [domain domain-id] vlan
```

- domain-id - An independent multicast domain. (Range: 1-5)
- vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

Default Setting
VLAN 1

Command Mode
Global Configuration

Command Usage
◆ This command specifies the VLAN through which MVR multicast data is received. This is the VLAN to which all source ports must be assigned.

◆ The VLAN specified by this command must be an existing VLAN configured with the vlan command.

◆ MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport native vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

Example
The following example sets the MVR VLAN to VLAN 2:

```
Console(config)#mvr
Console(config)#mvr domain 1 vlan 2
Console(config)#
```
### mvr immediate-leave
This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the `no` form to restore the default settings.

**Syntax**

```
[no] mvr [domain domain-id] immediate-leave [by-host-ip]
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
- `by-host-ip` - Specifies that the member port will be deleted only when there are no hosts joining this group.

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

- If the “by-host-ip” option is used, the router/querier will not send out a group-specific query when an IGMPv2/v3 leave message is received (the same as it would without this option having been used). Instead of immediately deleting that group, it will look up the record, and only delete the group if there are no other subscribers for it on the member port. Only when all hosts on that port leave the group will the member port be deleted.

- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

- Immediate leave does not apply to multicast groups which have been statically assigned to a port with the `mvr vlan group` command.

**Example**
The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 immediate-leave
Console(config-if)#
```
**mvr type**  This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

**Syntax**

```
[no] mvr [domain domain-id] type {receiver | source}
```

- **domain-id** - An independent multicast domain. (Range: 1-5)
- **receiver** - Configures the interface as a subscriber port that can receive multicast data.
- **source** - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

**Default Setting**
The port type is not defined.

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.

- Receiver ports can belong to different VLANs, but should not normally be configured as a member of the MVR VLAN. IGMP snooping can also be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see the switchport mode command).

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR protocol or which have been assigned through the `mvr vlan group` command.

- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the `mvr vlan group` command.

**Example**
The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
```
**mvr vlan group**  This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the no form to restore the default settings.

**Syntax**

\[
\text{[no]} \text{ mvr [domain domain-id] vlan vlan-id group ip-address}
\]

- **domain-id** - An independent multicast domain. (Range: 1-5)
- **vlan-id** - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)
- **group** - Defines a multicast service sent to the selected port.
- **ip-address** - Statically configures an interface to receive multicast traffic from the IPv4 address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

**Default Setting**
No receiver port is a member of any configured multicast group.

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
- Multicast groups can be statically assigned to a receiver port using this command.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.
- The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

**Example**
The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#mvr domain 1 vlan 3 group 225.0.0.5
Console(config-if)#
```
clear mvr groups
dynamic

This command clears multicast group information dynamically learned through MVR.

Syntax

clear mvr groups dynamic

Command Mode
Privileged Exec

Command Usage
This command only clears entries learned through MVR. Statically configured multicast address are not cleared.

Example

Console#clear mvr groups dynamic
Console#

clear mvr statistics

This command clears MVR statistics.

Syntax

clear mvr statistics [interface interface]

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)

vlan vlan-id - VLAN identifier (Range: 1-4094)

Command Mode
Privileged Exec

Example

Console#clear mvr statistics
Console#
**show mvr**  This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

**Syntax**

```
show mvr [domain domain-id]
```

*domain-id* - An independent multicast domain. (Range: 1-5)

**Default Setting**
Displays configuration settings for all MVR domains.

**Command Mode**
Privileged Exec

**Example**
The following shows the MVR settings:

```
Console#show mvr
MVR 802.1p Forwarding Priority : Disabled
MVR Proxy Switching : Enabled
MVR Robustness Value : 1
MVR Proxy Query Interval : 125(sec.)
MVR Source Port Mode : Always Forward
MVR Domain : 1
MVR Config Status : Enabled
MVR Running Status : Active
MVR Multicast VLAN : 1
MVR Current Learned Groups : 10
MVR Upstream Source IP : 192.168.0.3
```

**Table 123: show mvr - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR 802.1p Forwarding</td>
<td>Priority assigned to multicast traffic forwarded into the MVR VLAN Priority</td>
</tr>
<tr>
<td>Priority</td>
<td></td>
</tr>
<tr>
<td>MVR Proxy Switching</td>
<td>Shows if MVR proxy switching is enabled</td>
</tr>
<tr>
<td>MVR Robustness Value</td>
<td>Shows the number of reports or query messages sent when proxy switching is</td>
</tr>
<tr>
<td></td>
<td>enabled</td>
</tr>
<tr>
<td>MVR Proxy Query Interval</td>
<td>The interval at which the receiver port sends out general queries</td>
</tr>
<tr>
<td>MVR Source Port Mode</td>
<td>Shows if the switch only forwards multicast streams which the source port</td>
</tr>
<tr>
<td></td>
<td>has dynamically joined or always forwards multicast streams</td>
</tr>
<tr>
<td>MVR Domain</td>
<td>An independent multicast domain.</td>
</tr>
<tr>
<td>MVR Config Status</td>
<td>Shows if MVR is globally enabled on the switch.</td>
</tr>
<tr>
<td>MVR Running Status</td>
<td>Indicates whether or not all necessary conditions in the MVR environment</td>
</tr>
<tr>
<td></td>
<td>are satisfied. (Running status is true as long as MVR Status is enabled,</td>
</tr>
<tr>
<td></td>
<td>and the specified MVR VLAN exists.)</td>
</tr>
</tbody>
</table>
### show mvr associated-profile

This command shows the profiles bound the specified domain.

#### Syntax

```plaintext
show mvr [domain domain-id] associated-profile
```

*domain-id* - An independent multicast domain. (Range: 1-5)

#### Default Setting

Displays profiles bound to all MVR domains.

#### Command Mode

Privileged Exec

#### Example

The following displays the profiles bound to domain 1:

```
Console# show mvr domain 1 associated-profile
Domain ID : 1
MVR Profile Name     Start IP Addr.  End IP Addr.
-------------------- --------------- ---------------
rd                        228.1.23.1     228.1.23.10
testing                   228.2.23.1     228.2.23.10
Console#
```

### show mvr interface

This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

#### Syntax

```plaintext
show mvr [domain domain-id] interface
```

*domain-id* - An independent multicast domain. (Range: 1-5)

#### Default Setting

Displays configuration settings for all attached interfaces.

#### Command Mode

Privileged Exec

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Multicast VLAN</td>
<td>Shows the VLAN used to transport all MVR multicast traffic.</td>
</tr>
<tr>
<td>MVR Current Learned Groups</td>
<td>The current number of MVR group addresses</td>
</tr>
<tr>
<td>MVR Upstream Source IP</td>
<td>The source IP address assigned to all upstream control packets.</td>
</tr>
</tbody>
</table>
Example
The following displays information about the interfaces attached to the MVR VLAN in domain 1:

```
Console#show mvr domain 1 interface
MVR Domain : 1
Flag: H - immediate leave by host ip
Port Type Status Immediate Static Group Address
-------- -------- ------------------- ------------- ------------------------
Eth 1/ 1 Source Active/Forwarding
Eth 1/ 2 Receiver Inactive/Discarding Disabled 234.5.6.8(VLAN2)
Eth 1/ 3 Source Inactive/Discarding
Eth 1/ 1 Receiver Active/Forwarding Disabled 225.0.0.1(VLAN1)
225.0.0.9(VLAN3)
Eth1/ 4 Receiver Active/Discarding Disabled
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Domain</td>
<td>An independent multicast domain.</td>
</tr>
<tr>
<td>Port</td>
<td>Shows interfaces attached to the MVR.</td>
</tr>
<tr>
<td>Type</td>
<td>Shows the MVR port type.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the MVR status and interface status. MVR status for source ports is “ACTIVE” if MVR is globally enabled on the switch. MVR status for receiver ports is “ACTIVE” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface. Also shows if MVR traffic is being forwarded or discarded.</td>
</tr>
<tr>
<td>Immediate</td>
<td>Shows if immediate leave is enabled or disabled.</td>
</tr>
<tr>
<td>Static Group Address</td>
<td>Shows any static MVR group assigned to an interface, and the receiver VLAN.</td>
</tr>
</tbody>
</table>

show mvr members
This command shows information about the current number of entries in the forwarding database, detailed information about a specific multicast address, the IP address of the hosts subscribing to all active multicast groups, or the multicast groups associated with each port.

Syntax
```
show mvr [domain domain-id] members [ip-address | host-ip-address [interface] | igmp | sort-by-port [interface] | unknown | user]
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
- `ip-address` - IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- `members` - The multicast groups assigned to the MVR VLAN.
- `host-ip-address` - The subscriber IP addresses.
**Chapter 21 | Multicast Filtering Commands**

Multicast VLAN Registration for IPv4

- **igmp** - Entry created by IGMP protocol.
- **sort-by-port** - The multicast groups associated with an interface.
- **interface**
  - **ethernet unit/port**
    - **unit** - Unit identifier. (Range: 1)
    - **port** - Port number. (Range: 1-28/52)
  - **port-channel channel-id** (Range: 1-16)
- **unknown** - Entry created by receiving a multicast stream.
- **user** - Snooping entry learned from user's configuration settings.

**Default Setting**
Displays configuration settings for all domains and all forwarding entries.

**Command Mode**
Privileged Exec

**Example**
The following shows information about the number of multicast forwarding entries currently active in domain 1:

```
Console# show mvr domain 1 members
MVR Domain : 1
MVR Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
   H - Host counts (number of hosts joined to group on this port).
   P - Port counts (number of ports joined to group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address   VLAN Port        Up time     Expire Count
--------------- ---- ----------- ----------- ------ --------
234.5.6.7          1             00:00:09:17            2(P)
   1 Eth 1/ 1(S) 
   2 Eth 1/ 2(R) 

Console#
```

The following example shows detailed information about a specific multicast address:

```
Console# show mvr domain 1 members 234.5.6.7
MVR Domain : 1
MVR Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
   H - Host counts (number of hosts joined to group on this port).
   P - Port counts (number of ports joined to group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

234.5.6.7          1             00:00:09:17            2(P)
   1 Eth 1/ 1(S) 
   2 Eth 1/ 2(R) 

Console#
```
Table 125: show mvr members - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Multicast group address.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN to which this address is forwarded.</td>
</tr>
<tr>
<td>Port</td>
<td>Port to which this address is forwarded.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time that this multicast group has been known.</td>
</tr>
<tr>
<td>Expire</td>
<td>The time until this entry expires.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of times this address has been learned by IGMP snooping.</td>
</tr>
</tbody>
</table>

**show mvr profile**  
This command shows all configured MVR profiles.

**Command Mode**  
Privileged Exec

**Example**  
The following shows all configured MVR profiles:

```
Console#show mvr profile
MVR Profile Name     Start IP Addr.  End IP Addr.
--------------------- --------------- ---------------
rd                    228.1.23.1     228.1.23.10
testing               228.2.23.1     228.2.23.10
Console#
```

**show mvr statistics**  
This command shows MVR protocol-related statistics for the specified interface.

**Syntax**

```
show mvr [domain domain-id] statistics
```

*domain-id* - An independent multicast domain. (Range: 1-5)
interface
  **ethernet** unit/port
  
  *unit* - Unit identifier. (Range: 1)
  *port* - Port number. (Range: 1-28/52)

  **port-channel** channel-id (Range: 1-16)

  **vlan** vlan-id - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.
summary - Displays summary of MVR statistics.
mvr vlan - Displays summary statistics for the MVR VLAN.

**Default Setting**
Displays statistics for all domains.

**Command Mode**
Privileged Exec

**Example**
The following shows MVR protocol-related statistics received:

```
Console#show mvr domain 1 statistics input
MVR Domain : 1 , MVR VLAN: 2
Input Statistics:
  Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
  --------- -------- -------- -------- ------------- -------- --------- ------
  Eth 1/ 1        23       11        4            10        5        20      9
  Eth 1/ 2        12       15        8             3        5        19      4
  DVLAN   1        2        0        0             2        2        20      9
  MVLAN   1        2        0        0             2        2        20      9
Console#
```

**Table 126: show mvr statistics input - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows interfaces attached to the MVR.</td>
</tr>
<tr>
<td>Report</td>
<td>The number of IGMP membership reports received on this interface.</td>
</tr>
<tr>
<td>Leave</td>
<td>The number of leave messages received on this interface.</td>
</tr>
<tr>
<td>G Query</td>
<td>The number of general query messages received on this interface.</td>
</tr>
<tr>
<td>G(-S)-S Query</td>
<td>The number of group specific or group-and-source specific query messages received on this interface.</td>
</tr>
<tr>
<td>Drop</td>
<td>The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received</td>
</tr>
<tr>
<td>Join Succ</td>
<td>The number of times a multicast group was successfully joined.</td>
</tr>
<tr>
<td>Group</td>
<td>The number of MVR groups active on this interface.</td>
</tr>
</tbody>
</table>
The following shows MVR protocol-related statistics sent:

```
Console#show mvr domain 1 statistics output
MVR Domain : 1 , MVR VLAN: 2
Output Statistics:
<table>
<thead>
<tr>
<th>Interface</th>
<th>Report</th>
<th>Leave</th>
<th>G Query</th>
<th>G(-S)-S Query</th>
<th>Drop</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/1</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DVLAN 1</td>
<td>7</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MVLAN 1</td>
<td>7</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

```
Table 127: show mvr statistics output - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows interfaces attached to the MVR.</td>
</tr>
<tr>
<td>Report</td>
<td>The number of IGMP membership reports sent from this interface.</td>
</tr>
<tr>
<td>Leave</td>
<td>The number of leave messages sent from this interface.</td>
</tr>
<tr>
<td>G Query</td>
<td>The number of general query messages sent from this interface.</td>
</tr>
<tr>
<td>G(-S)-S Query</td>
<td>The number of group specific or group-and-source specific query messages sent from this interface.</td>
</tr>
<tr>
<td>Drop</td>
<td>The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.</td>
</tr>
<tr>
<td>Group</td>
<td>The number of multicast groups active on this interface.</td>
</tr>
</tbody>
</table>
```

The following shows MVR query-related statistics:

```
Console#show mvr domain 1 statistics query
Domain 1:
Other Querier          : None
Other Querier Expire   : 0(m):0(s)
Other Querier Uptime    : 0(h):0(m):0(s)
Self Querier           : None
Self Querier Expire    : 0(m):30(s)
Self Querier Uptime     : 0(h):30(m):55(s)
General Query Received  : 0
General Query Sent      : 8
Specific Query Received : 0
Specific Query Sent     : 3
Warn Rate Limit         : 0 sec.
V1 Warning Count        : 0
V2 Warning Count        : 0
V3 Warning Count        : 0
```

---

- 650 -
The following shows MVR summary statistics for an interface:

```
Console#show mvr domain 1 statistics summary interface ethernet 1/1
Domain 1:
Number of Groups: 0
Querier: Report & Leave: 
Transmit: Transmit : 7
General: Report : 0
Group Specific: Leave : 4
Received: Recieved :
General: Report : 0
Group Specific: Leave : 0
V1 Warning Count: 0
V2 Warning Count: 0
V3 Warning Count: 0
Source Port Drop : 0
Others Drop : 0
Console#
```

Table 128: show mvr statistics query - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Querier</td>
<td>The IP address of the querier on this interface.</td>
</tr>
<tr>
<td>Other Querier Expire</td>
<td>The time after which this querier is assumed to have expired.</td>
</tr>
<tr>
<td>Other Querier Uptime</td>
<td>Other querier's time up.</td>
</tr>
<tr>
<td>Self Querier</td>
<td>This querier's IP address.</td>
</tr>
<tr>
<td>Self Querier Expire</td>
<td>This querier's expire time.</td>
</tr>
<tr>
<td>Self Querier Uptime</td>
<td>This querier's time up.</td>
</tr>
<tr>
<td>General Query Received</td>
<td>The number of general queries received on this interface.</td>
</tr>
<tr>
<td>General Query Sent</td>
<td>The number of general queries sent from this interface.</td>
</tr>
<tr>
<td>Specific Query Received</td>
<td>The number of specific queries received on this interface.</td>
</tr>
<tr>
<td>Specific Query Sent</td>
<td>The number of specific queries sent from this interface.</td>
</tr>
<tr>
<td>Warn Rate Limit</td>
<td>Count down from 15 seconds after receiving a Query different from the configured version.</td>
</tr>
<tr>
<td>V# Warning Count</td>
<td>Number of queries received on MVR that were configured for IGMP version 1, 2 or 3.</td>
</tr>
</tbody>
</table>

Table 129: show mvr statistics summary interface - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>An independent multicast domain.</td>
</tr>
<tr>
<td>Number of Groups</td>
<td>Number of groups learned on this port.</td>
</tr>
<tr>
<td>Querier</td>
<td></td>
</tr>
<tr>
<td>Transmit</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>Number of general queries transmitted.</td>
</tr>
<tr>
<td>Group Specific</td>
<td>Number of group specific queries transmitted.</td>
</tr>
</tbody>
</table>
The following shows MVR summary statistics for the MVR VLAN:

```
Console#show mvr domain 1 statistics summary interface mvr-vlan
Domain 1:
Number of Groups: 0
Querier: : Report & Leave: :
  Other Querier : None Host IP Addr : 192.168.0.66
  Other Expire : 0(m):0(s) Unsolicit Expire : 5(m):4(s)
  Other Uptime : 0(h):0(m):0(s)
Self Querier : None
Self Expire : 1(m):45(s)
Self Uptime : 0(h):14(m):54(s)
Transmit : Transmit :
  General : 11 Report : 7
  Group Specific : 3 Leave : 4
Received : Received :
  General : 0 Report : 6
  Group Specific : 0 Leave : 0
V1 Warning Count: 0 Join Success : 6
V2 Warning Count: 0 Filter Drop : 0
V3 Warning Count: 0
  Source Port Drop: 0
  Others Drop : 0
Console#
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>An independent multicast domain.</td>
</tr>
<tr>
<td>Number of Groups</td>
<td>Number of groups learned on this port.</td>
</tr>
<tr>
<td>Querier</td>
<td></td>
</tr>
<tr>
<td>Other Querier</td>
<td>Other IGMP querier's IP address.</td>
</tr>
<tr>
<td>Other Expire</td>
<td>Other querier’s expire time.</td>
</tr>
<tr>
<td>Other Uptime</td>
<td>Other querier’s time up.</td>
</tr>
<tr>
<td>Self Querier</td>
<td>This querier’s IP address.</td>
</tr>
<tr>
<td>Self Expire</td>
<td>This querier’s expire time.</td>
</tr>
<tr>
<td>Self Uptime</td>
<td>This querier’s time up.</td>
</tr>
<tr>
<td>Transmit</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>Number of general queries sent from receiver port.</td>
</tr>
<tr>
<td>Group Specific</td>
<td>Number of group specific queries sent from receiver port.</td>
</tr>
<tr>
<td>Received</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>Number of general queries received.</td>
</tr>
<tr>
<td>Group Specific</td>
<td>Number of group specific queries received.</td>
</tr>
<tr>
<td>V# Warning Count</td>
<td>Number of queries received on MVR that were configured by IGMP version 1, 2 or 3.</td>
</tr>
<tr>
<td>Report &amp; Leave</td>
<td></td>
</tr>
<tr>
<td>Host IP Addr</td>
<td>Source IP address used to send report/leave messages from source port.</td>
</tr>
<tr>
<td>Unsolicit Expire</td>
<td>Expiration time for unsolicit reports sent out from source port</td>
</tr>
<tr>
<td>Transmit</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Number of reports sent out from source port.</td>
</tr>
<tr>
<td>Leave</td>
<td>Number of leaves sent out from source port.</td>
</tr>
<tr>
<td>Received</td>
<td>Field header</td>
</tr>
<tr>
<td>Report</td>
<td>Number of reports received.</td>
</tr>
<tr>
<td>Leave</td>
<td>Number of leaves received.</td>
</tr>
<tr>
<td>Join Success</td>
<td>Number of join reports processed successfully.</td>
</tr>
<tr>
<td>Filter Drop</td>
<td>Number of report/leave messages dropped by IGMP filter.</td>
</tr>
<tr>
<td>Source Port Drop</td>
<td>Number of report/leave messages dropped by MVR source port.</td>
</tr>
<tr>
<td>Others Drop</td>
<td>Number of report/leave messages dropped for other reasons.</td>
</tr>
</tbody>
</table>
Multicast VLAN Registration for IPv6

This section describes commands used to configure Multicast VLAN Registration for IPv6 (MVR6). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider’s network. Any multicast traffic entering an MVR6 VLAN is sent to all subscribers. This can significantly reduce the processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR6 maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 131: Multicast VLAN Registration for IPv6 Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mvr6 associated-profile</td>
<td>Binds the MVR6 group addresses specified in a profile to an MVR6 domain</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 domain</td>
<td>Enables MVR6 for a specific domain</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 priority</td>
<td>Assigns a priority to all multicast traffic in the MVR6 VLAN</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 profile</td>
<td>Maps a range of MVR6 group addresses to a profile</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 proxy-query-interval</td>
<td>Configures the interval at which the receiver port sends out general queries.</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 proxy-switching</td>
<td>Enables MVR6 proxy switching, where the source port acts as a host, and the receiver port acts as an MVR6 router with querier service enabled</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 robustness-value</td>
<td>Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 source-port-mode dynamic</td>
<td>Configures the switch to only forward multicast streams which the source port has dynamically joined</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 upstream-source-ip</td>
<td>Configures the source IP address assigned to all control packets sent upstream</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 vlan</td>
<td>Specifies the VLAN through which MVR6 multicast data is received</td>
<td>GC</td>
</tr>
<tr>
<td>mvr6 immediate-leave</td>
<td>Enables immediate leave capability</td>
<td>IC</td>
</tr>
<tr>
<td>mvr6 type</td>
<td>Configures an interface as an MVR6 receiver or source port</td>
<td>IC</td>
</tr>
<tr>
<td>mvr6 vlan group</td>
<td>Statically binds a multicast group to a port</td>
<td>IC</td>
</tr>
<tr>
<td>clear mvr6 groups dynamic</td>
<td>Clears multicast group information dynamically learned through MVR6</td>
<td>PE</td>
</tr>
<tr>
<td>clear mvr6 statistics</td>
<td>Clears the MVR6 statistics globally or on a per-interface basis.</td>
<td>PE</td>
</tr>
<tr>
<td>show mvr6</td>
<td>Shows information about MVR6 domain settings, including MVR6 operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address</td>
<td>PE</td>
</tr>
<tr>
<td>show mvr6 associated-profile</td>
<td>Shows the profiles bound the specified domain</td>
<td>PE</td>
</tr>
<tr>
<td>show mvr6 interface</td>
<td>Shows MVR6 settings for interfaces attached to the MVR6 VLAN</td>
<td>PE</td>
</tr>
</tbody>
</table>
Table 131: Multicast VLAN Registration for IPv6 Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mvr6 members</td>
<td>Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address</td>
<td>PE</td>
</tr>
<tr>
<td>show mvr6 profile</td>
<td>Shows all configured MVR6 profiles</td>
<td>PE</td>
</tr>
<tr>
<td>show mvr6 statistics</td>
<td>Shows MVR6 protocol statistics for the specified interface</td>
<td>PE</td>
</tr>
</tbody>
</table>

mvr6 associated-profile

This command binds the MVR6 group addresses specified in a profile to an MVR6 domain. Use the **no** form of this command to remove the binding.

Syntax

```plaintext
[no] mvr6 domain domain-id associated-profile profile-name
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
- `profile-name` - The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

Example

The following an MVR6 group address profile to domain 1:

```plaintext
Console(config)#mvr6 domain 1 associated-profile rd
Console(config)#
```

mvr6 domain

This command enables Multicast VLAN Registration for IPv6 (MVR6) for a specific domain. Use the **no** form of this command to disable MVR6 for a domain.

Syntax

```plaintext
[no] mvr6 domain domain-id
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
When MVR6 is enabled on a domain, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group.

Example
The following example enables MVR6 for domain 1:

```
Console(config)#mvr6 domain 1
Console(config)#
```

mvr6 priority
This command assigns a priority to all multicast traffic in the MVR6 VLAN. Use the no form of this command to restore the default setting.

Syntax
```
mvr6 priority priority
no mvr6 priority
```

- `priority` - The CoS priority assigned to all multicast traffic forwarded into the MVR6 VLAN. (Range: 0-7, where 7 is the highest priority)

Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

Example
```
Console(config)#mvr6 priority 6
Console(config)#
```

Related Commands
show mvr6
This command maps a range of MVR6 group addresses to a profile. Use the no form of this command to remove the profile.

Syntax

```
mvr6 profile profile-name start-ip-address end-ip-address
```

- `profile-name` - The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)
- `start-ip-address` - Starting IPv6 address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- `end-ip-address` - Ending IPv6 address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Setting

No profiles are defined

Command Mode

Global Configuration

Command Usage

- Use this command to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

- IGMP snooping and MVR6 share a maximum number of 1023 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

- The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

Example

The following example maps a range of MVR6 group addresses to a profile:

```
Console(config)#mvr6 profile rd ff01::0:0:0:fe ff01::0:0:0:ff
Console(config)#
```
**mvr6 proxy-query-interval**

This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

**Syntax**

```
mvr6 proxy-query-interval interval
no mvr6 proxy-query-interval
```

- **interval** - The interval at which the receiver port sends out general queries.
  (Range: 2-31744 seconds)

**Default Setting**

125 seconds

**Command Mode**

Global Configuration

**Command Usage**

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the **mvr6 proxy-switching** command.

**Example**

This example sets the proxy query interval for MVR6.

```
Console(config)#mvr6 proxy-query-interval 1000
Console(config)#
```

---

**mvr6 proxy-switching**

This command enables MVR6 proxy switching, where the source port acts as a host, and the receiver port acts as an MVR6 router with querier service enabled. Use the **no** form to disable this function.

**Syntax**

```
[no] mvr6 proxy-switching
```

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Command Usage**

- When MVR6 proxy-switching is enabled, an MVR6 source port serves as the upstream or host interface, and the MVR6 receiver port serves as the querier. The source port performs only the host portion of MVR6 by sending summarized membership reports, and automatically disables MVR6 router functions.
Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR6 router functions by maintaining a database of all MVR6 subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR6 proxy service.

When the source port receives report and leave messages, it only forwards them to other source ports.

When receiver ports receive any query messages, they are dropped.

When changes occurring in the downstream MVR6 groups are learned by the receiver ports through report and leave messages, an MVR6 state change report is created and sent to the upstream source port, which in turn forwards this information upstream.

When MVR6 proxy switching is disabled:

- Any membership reports received from receiver/source ports are forwarded to all source ports.
- When a source port receives a query message, it will be forwarded to all downstream receiver ports.
- When a receiver port receives a query message, it will be dropped.

**Example**
The following example enable MVR6 proxy switching.

```
Console(config)#mvr6 proxy-switching
Console(config)#
```

**Related Commands**

`mvr6 robustness-value (659)`

This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the `no` form to restore the default setting.

**Syntax**

```
mvr6 robustness-value value
no mvr6 robustness-value
```

`value` - The robustness used for all interfaces. (Range: 1-10)

**Default Setting**

2
Chapter 21 | Multicast Filtering Commands
Multicast VLAN Registration for IPv6

Command Mode
Global Configuration

Command Usage
◆ This command sets the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.

◆ This command only takes effect when MVR6 proxy switching is enabled.

Example

```
Console(config)#mvr6 robustness-value 5
Console(config)#
```

Related Commands
mvr6 proxy-switching (658)

mvr6 source-port-mode dynamic
This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

Syntax

```
[no] mvr6 source-port-mode dynamic
```

Default Setting
Forwards all multicast streams which have been specified in a profile and bound to a domain.

Command Mode
Global Configuration

Command Usage
◆ By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

◆ When the **mvr6 source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.
Example

```console
Console(config)#mvr6 source-port-mode dynamic
Console(config)#
```

**mvr6 upstream-source-ip**

This command configures the source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. Use the no form to restore the default setting.

**Syntax**

```text
mvr6 domain domain-id upstream-source-ip source-ip-address
no mvr6 domain domain-id upstream-source-ip
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
- `source-ip-address` – The source IPv6 address assigned to all MVR6 control packets sent upstream. This parameter must be a full IPv6 address including the network prefix and host address bits.

**Default Setting**

All MVR6 reports sent upstream use a null source IP address.

**Command Mode**

Global Configuration

**Command Usage**

All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

Example

```console
Console(config)#mvr6 domain 1 upstream-source-ip 2001:DB8:2222:7223::72
Console(config)#
```

**mvr6 vlan**

This command specifies the VLAN through which MVR6 multicast data is received. Use the no form of this command to restore the default MVR6 VLAN.

**Syntax**

```text
mvr6 domain domain-id vlan vlan-id
no mvr6 domain domain-id vlan
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
**vlan-id** - Specifies the VLAN through which MVR6 multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

**Default Setting**
VLAN 1

**Command Mode**
Global Configuration

**Command Usage**
MVR6 source ports can be configured as members of the MVR6 VLAN using the `switchport allowed vlan` command and `switchport native vlan` command, but MVR6 receiver ports should not be statically configured as members of this VLAN.

**Example**
The following example sets the MVR6 VLAN to VLAN 1:

```
Console(config)#mvr6 domain 1 vlan 1
Console(config)#
```

**mvr6 immediate-leave**
This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the `no` form to restore the default settings.

**Syntax**
```
[no] mvr6 domain domain-id immediate-leave [by-host-ip]
```

- `domain-id` - An independent multicast domain. (Range: 1-5)
- `by-host-ip` - Specifies that the member port will be deleted only when there are no hosts joining this group.

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
If the “by-host-ip” option is used, the router/querier will not send out a group-specific query when an MLDv1/v2 Listener Done message is received (the same as it would without this option having been used). Instead of immediately deleting that group, it will look up the record, and only delete the group if there are no other subscribers for it on the member port. Only when all hosts on that port leave the group will the member port be deleted.

Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

Immediate leave does not apply to multicast groups which have been statically assigned to a port with the `mvr6 vlan group` command.

**Example**
The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 immediate-leave
Console(config-if)#
```

**mvr6 type**
This command configures an interface as an MVR6 receiver or source port. Use the `no` form to restore the default settings.

**Syntax**

```
[no] mvr6 domain domain-id type {receiver | source}
```

domain-id - An independent multicast domain. (Range: 1-5)
receiver - Configures the interface as a subscriber port that can receive multicast data.
source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups. Note that the source port must be manually configured as a member of the MVR6 VLAN using the `switchport allowed vlan` command.

**Default Setting**
The port type is not defined.

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
- A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6. A port which is not configured as an MVR6 receiver or source port can use MLD snooping to join or leave multicast groups using the standard rules for multicast filtering (see “MLD Snooping” on page 608).
Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR6 VLAN. MLD snooping can be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR6 VLAN. Also, note that VLAN membership for MVR6 receiver ports cannot be set to access mode (see the `switchport mode` command).

One or more interfaces may be configured as MVR6 source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR6 protocol or which have been assigned through the `mvr6 vlan group` command.

All source ports must belong to the MVR6 VLAN.

Subscribers should not be directly connected to source ports.

The same port cannot be configured as a source port in one MVR6 domain and as a receiver port in another domain.

### Example

The following configures one source port and several receiver ports on the switch.

```bash
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#
```

### mvr6 vlan group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

#### Syntax

```bash
[no] mvr6 domain domain-id vlan vlan-id group ip-address

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv6 address specified for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
```

#### Default Setting

No receiver port is a member of any configured multicast group.
Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ Multicast groups can be statically assigned to a receiver port using this command. The assigned address must fall within the range set by the mvr6 associated-profile command.

◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

◆ The MVR6 VLAN cannot be specified as the receiver VLAN for static bindings.

Example
The following statically assigns a multicast group to a receiver port:

```console
Console(config)#interface ethernet 1/2
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1
Console(config-if)#
```

clear mvr6 groups dynamic
This command clears multicast group information dynamically learned through MVR6.

Syntax
```
clear mvr6 groups dynamic [domain domain-id]
```

domain-id - An independent multicast domain. (Range: 1-5)

Command Mode
Privileged Exec

Command Usage
This command only clears entries learned though MVR6. Statically configured multicast addresses are not cleared.

Example
```
Console#clear mvr6 groups dynamic
Console#
```
clear mvr6 statistics  Use this command to clear the MVR6 statistics.

Syntax

```
clear mvr6 statistics [interface {ethernet unit/port | port-channel channel-id | vlan vlan-id}]
```

- **ethernet** unit/port
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)
- **port-channel** channel-id (Range: 1-16)
- **vlan** vlan-id (Range: 1-4094)

**Command Mode**
Privileged Exec

**Command Usage**
If the interface option is not used then all MVR6 statistics are cleared. Otherwise using the interface option will only clear the MVR6 statistics of the specified interface.

**Example**
The following shows how to clear all the MVR6 statistics:

```
Console#clear mvr6 statistics
Console#
```

show mvr6  This command shows information about MVR6 domain settings, including MVR6 operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

Syntax

```
show mvr6 [domain domain-id]
```

- **domain-id** - An independent multicast domain. (Range: 1-5)

**Default Setting**
Displays configuration settings for all MVR6 domains.

**Command Mode**
Privileged Exec
Example
The following shows the MVR6 settings:

```
Console# show mvr6
MVR6 802.1p Forwarding Priority: Disabled
MVR6 Proxy Switching : Enabled
MVR6 Robustness Value : 2
MVR6 Proxy Query Interval : 125(sec.)
MVR6 Source Port Mode : Always Forward

Domain : 1
MVR6 Config Status : Enabled
MVR6 Running Status : Active
MVR6 Multicast VLAN : 1
MVR6 Current Learned Groups : 0
MVR6 Upstream Source IP : FF05::25
```

Table 132: show mvr6 - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR6 802.1p Forwarding Priority</td>
<td>Priority assigned to multicast traffic forwarded into the MVR6 VLAN</td>
</tr>
<tr>
<td>MVR6 Proxy Switching</td>
<td>Shows if MVR6 proxy switching is enabled</td>
</tr>
<tr>
<td>MVR6 Robustness Value</td>
<td>Shows the number of reports or query messages sent when proxy switching is enabled</td>
</tr>
<tr>
<td>MVR6 Proxy Query Interval</td>
<td>The interval at which the receiver port sends out general queries</td>
</tr>
<tr>
<td>MVR6 Source Port Mode</td>
<td>Shows if the switch only forwards multicast streams which the source port has dynamically joined or always forwards multicast streams</td>
</tr>
<tr>
<td>MVR6 Domain</td>
<td>An independent multicast domain.</td>
</tr>
<tr>
<td>MVR6 Config Status</td>
<td>Shows if MVR6 is globally enabled on the switch.</td>
</tr>
<tr>
<td>MVR6 Running Status</td>
<td>Indicates whether or not all necessary conditions in the MVR6 environment are satisfied. (Running status is true as long as MVR6 Status is enabled, and the specified MVR6 VLAN exists, and a source port with a valid link has been configured (using the mvr6 type command.)</td>
</tr>
<tr>
<td>MVR6 Multicast VLAN</td>
<td>Shows the VLAN used to transport all MVR6 multicast traffic.</td>
</tr>
<tr>
<td>MVR6 Upstream Source IP</td>
<td>The source IP address assigned to all upstream control packets.</td>
</tr>
</tbody>
</table>

**show mvr6 associated-profile**

This command shows the profiles bound the specified domain.

**Syntax**

```
show mvr6 [domain domain-id] associated-profile
```

`domain-id` - An independent multicast domain. (Range: 1-5)

**Default Setting**

Displays profiles bound to all MVR6 domains.
Command Mode
Privileged Exec

Example
The following displays the profiles bound to domain 1:

```
Console#show mvr6 domain 1 associated-profile
Domain ID : 1
MVR6 Profile Name     Start IPv6 Addr.          End IPv6 Addr.
-------------------- ------------------------- -------------------------
C rd                                   ff01::fe                  ff01::ff
Console#
```

show mvr6 interface  This command shows MVR6 configuration settings for interfaces attached to the MVR6 VLAN.

Syntax
```
show mvr6 [domain domain-id] interface
```

- `domain domain-id` - An independent multicast domain. (Range: 1-5)

Default Setting
Displays configuration settings for all attached interfaces.

Command Mode
Privileged Exec

Example
The following displays information about the interfaces attached to the MVR6 VLAN in domain 1:

```
Console#show mvr6 domain 1 interface
MVR6 Domain : 1
Port     Type          Status               Immediate Leave Static Group Address
-------- -------- ------------------- ---------------- ---------------------
Eth1/1  Source     Active/Forwarding
Eth1/2  Receiver  Active/Forwarding  Disabled          ff00::1(VLAN2)
Console#
```

Table 133: show mvr6 interface - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Shows interfaces attached to the MVR6.</td>
</tr>
<tr>
<td>Type</td>
<td>Shows the MVR6 port type.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the MVR6 status and interface status. MVR6 status for source ports is “ACTIVE” if MVR6 is globally enabled on the switch. MVR6 status for receiver ports is “ACTIVE” only if there are subscribers receiving multicast traffic from one of the MVR6 groups, or a multicast group has been statically assigned to an interface.</td>
</tr>
</tbody>
</table>
show mvr6 members

This command shows information about the current number of entries in
the forwarding database, or detailed information about a specific multicast
address.

Syntax

```
show mvr6 [domain domain-id] members [ip-address]
```

domain-id - An independent multicast domain. (Range: 1-5)
ip-address - IPv6 address for an MVR6 multicast group.

Default Setting
Displays configuration settings for all domains and all forwarding entries.

Command Mode
Privileged Exec

Example
The following shows information about the number of multicast forwarding
entries currently active in domain 1:

```
Console#show mvr6 domain 1 members
MVR6 Domain : 1
MVR6 Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
    H - Host counts (number of hosts join the group on this port).
    P - Port counts (number of forwarding ports).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

<table>
<thead>
<tr>
<th>Group Address</th>
<th>VLAN</th>
<th>Port</th>
<th>Up time</th>
<th>Expire Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::101</td>
<td>2</td>
<td>Eth1</td>
<td>00:00:00:19</td>
<td>2 (P)</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Eth1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Eth1</td>
<td></td>
<td>0 (H)</td>
</tr>
</tbody>
</table>
```

Table 133: show mvr6 interface - display description (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate</td>
<td>Shows if immediate leave is enabled or disabled.</td>
</tr>
<tr>
<td>Static Group Address</td>
<td>Shows any static MVR6 group assigned to an interface, and the receiver VLAN.</td>
</tr>
</tbody>
</table>
The following example shows detailed information about a specific multicast address:

```
Console#show mvr6 domain 1 members ff00::1
MVR6 Domain : 1
MVR6 Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
        H - Host counts (number of hosts join the group on this port).
        P - Port counts (number of forwarding ports).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

<table>
<thead>
<tr>
<th>Group Address</th>
<th>VLAN</th>
<th>Port</th>
<th>Up time</th>
<th>Expire</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::101</td>
<td>2</td>
<td>Eth1/</td>
<td>00:00:03:18</td>
<td>2</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 (S)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Eth1/4 (R)</td>
<td></td>
<td>0</td>
<td>H</td>
</tr>
</tbody>
</table>

Console#
```

### Table 134: show mvr6 members - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Multicast group address.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN to which this address is forwarded.</td>
</tr>
<tr>
<td>Port</td>
<td>Port to which this address is forwarded.</td>
</tr>
<tr>
<td>Up time</td>
<td>Time that this multicast group has been known.</td>
</tr>
<tr>
<td>Expire</td>
<td>The time until this entry expires.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of times this address has been learned by MVR6 (MLD snooping).</td>
</tr>
</tbody>
</table>

**show mvr6 profile**

This command shows all configured MVR6 profiles.

**Command Mode**

Privileged Exec

**Example**

The following shows all configured MVR6 profiles:

```
Console#show mvr6 profile
MVR6 Profile Name | Start IPv6 Addr. | End IPv6 Addr.|
------------------|------------------|---------------|
rd                | ff01::fe         | ff01::ff      |
Console#
```
show mvr6 statistics

This command shows MVR protocol-related statistics for the specified interface.

Syntax

show mvr6 statistics {input | output} [interface interface]
show mvr6 domain domain-id statistics {input [interface interface] | output [interface interface] | query}

  domain-id - An independent multicast domain. (Range: 1-5)

  interface

    ethernet unit/port

      unit - Unit identifier. (Range: 1)

      port - Port number. (Range: 1-28/52)

  port-channel channel-id (Range: 1-16)

  vlan vlan-id - VLAN ID (Range: 1-4094)

  query - Displays MVR query-related statistics.

Default Setting

Displays statistics for all domains.

Command Mode

Privileged Exec

Example

The following shows MVR6 protocol-related statistics received:

```
Console#show mvr6 domain 1 statistics input
MVR6 Domain 1, MVR6 VLAN 2:
Input Statistics:

    Interface Report  Leave  G Query  G(-S)-S Query  Drop  Join Succ  Group
    ----  --------  --------  -----------  ------  --------  -----
     Eth 1/ 1    23       11        4            10       5        20     9
     Eth 1/ 2    12       15        8            3         5        19     4
    DVLAN    1       2        0          0            2         2       20     9
    MVLAN    2       2        0          0            2         2       20     9
Console#
```

Table 135: show mvr6 statistics input - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows interfaces attached to the MVR.</td>
</tr>
<tr>
<td>Report</td>
<td>The number of IGMP membership reports received on this interface.</td>
</tr>
<tr>
<td>Leave</td>
<td>The number of leave messages received on this interface.</td>
</tr>
<tr>
<td>G Query</td>
<td>The number of general query messages received on this interface.</td>
</tr>
</tbody>
</table>
The following shows MVR6 protocol-related statistics sent:

```
Console#show mvr6 domain 1 statistics output
MVR6 Domain 1, MVR6 VLAN 2:
Output Statistics:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Report</th>
<th>Done</th>
<th>G Query</th>
<th>G(-S)-S Query</th>
<th>Drop</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Eth 1/3</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DVLAN 1</td>
<td>7</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MVLAN 2</td>
<td>7</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Console#
```

Table 136: show mvr6 statistics output - display description (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows interfaces attached to the MVR.</td>
</tr>
<tr>
<td>Report</td>
<td>The number of IGMP membership reports sent from this interface.</td>
</tr>
<tr>
<td>Leave</td>
<td>The number of leave messages sent from this interface.</td>
</tr>
<tr>
<td>G Query</td>
<td>The number of general query messages sent from this interface.</td>
</tr>
<tr>
<td>G(-S)-S Query</td>
<td>The number of group specific or group-and-source specific query messages sent from this interface.</td>
</tr>
<tr>
<td>Group</td>
<td>The number of MVR groups active on this interface.</td>
</tr>
</tbody>
</table>

The following shows MVR6 query-related statistics:

```
Console#show mvr6 domain 1 statistics query
Other Querier Address   : fe80::2e0:0:0:fe00:fb/64
Other Querier Uptime    : 0(h):0(m):0(s)
Other Querier Expire Time: 0(m):0(s)
Self Querier Address    : None
Self Querier Uptime     : 0(h):13(m):16(s)
Self Querier Expire Time: 3(m):23(s)
General Query Received  : 0
General Query Sent       : 0
Specific Query Received  : 0
Specific Query Sent      : 0

Console#
```
LLDP Commands

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 137: LLDP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp</td>
<td>Enables LLDP globally on the switch</td>
<td>GC</td>
</tr>
<tr>
<td>lldp holdtime-multiplier</td>
<td>Configures the time-to-live (TTL) value sent in LLDP advertisements</td>
<td>GC</td>
</tr>
<tr>
<td>lldp med-fast-start-count</td>
<td>Configures how many medFastStart packets are transmitted</td>
<td>GC</td>
</tr>
<tr>
<td>lldp notification-interval</td>
<td>Configures the allowed interval for sending SNMP notifications about LLDP changes</td>
<td>GC</td>
</tr>
<tr>
<td>lldp refresh-interval</td>
<td>Configures the periodic transmit interval for LLDP advertisements</td>
<td>GC</td>
</tr>
<tr>
<td>lldp reinit-delay</td>
<td>Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down</td>
<td>GC</td>
</tr>
<tr>
<td>lldp tx-delay</td>
<td>Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables</td>
<td>GC</td>
</tr>
<tr>
<td>lldp admin-status</td>
<td>Enables LLDP transmit, receive, or transmit and receive mode on the specified port</td>
<td>IC</td>
</tr>
<tr>
<td>lldp basic-tlv management-ip-address</td>
<td>Configures an LLDP-enabled port to advertise the management address for this device</td>
<td>IC</td>
</tr>
<tr>
<td>lldp basic-tlv port-description</td>
<td>Configures an LLDP-enabled port to advertise its port description</td>
<td>IC</td>
</tr>
<tr>
<td>lldp basic-tlv system-capabilities</td>
<td>Configures an LLDP-enabled port to advertise its system capabilities</td>
<td>IC</td>
</tr>
<tr>
<td>lldp basic-tlv system-description</td>
<td>Configures an LLDP-enabled port to advertise the system description</td>
<td>IC</td>
</tr>
<tr>
<td>Command</td>
<td>Function</td>
<td>Mode</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>lldp basic-tlv system-name</td>
<td>Configures an LLDP-enabled port to advertise its system name</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot1-tlv proto-ident*</td>
<td>Configures an LLDP-enabled port to advertise the supported protocols</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot1-tlv proto-vid*</td>
<td>Configures an LLDP-enabled port to advertise port related VLAN information</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot1-tlv pvid*</td>
<td>Configures an LLDP-enabled port to advertise its default VLAN ID</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot1-tlv vlan-name*</td>
<td>Configures an LLDP-enabled port to advertise its VLAN name</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot3-tlv link-agg</td>
<td>Configures an LLDP-enabled port to advertise its link aggregation capabilities</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot3-tlv mac-phy</td>
<td>Configures an LLDP-enabled port to advertise its MAC and physical layer specifications</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot3-tlv max-frame</td>
<td>Configures an LLDP-enabled port to advertise its maximum frame size</td>
<td>IC</td>
</tr>
<tr>
<td>lldp dot3-tlv poe</td>
<td>Configures an LLDP-enabled port to advertise its Power-over-Ethernet capabilities</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-location civic-addr</td>
<td>Configures an LLDP-MED-enabled port to advertise its location identification details</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-notification</td>
<td>Enables the transmission of SNMP trap notifications about LLDP-MED changes</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-tlv ext-poe</td>
<td>Configures an LLDP-MED-enabled port to advertise its extended Power over Ethernet configuration and usage information</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-tlv inventory</td>
<td>Configures an LLDP-MED-enabled port to advertise its inventory identification details</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-tlv location</td>
<td>Configures an LLDP-MED-enabled port to advertise its location identification details</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-tlv med-cap</td>
<td>Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities</td>
<td>IC</td>
</tr>
<tr>
<td>lldp med-tlv network-policy</td>
<td>Configures an LLDP-MED-enabled port to advertise its network policy configuration</td>
<td>IC</td>
</tr>
<tr>
<td>lldp notification</td>
<td>Enables the transmission of SNMP trap notifications about LLDP changes</td>
<td>IC</td>
</tr>
<tr>
<td>show lldp config</td>
<td>Shows LLDP configuration settings for all ports</td>
<td>PE</td>
</tr>
<tr>
<td>show lldp info local-device</td>
<td>Shows LLDP global and interface-specific configuration settings for this device</td>
<td>PE</td>
</tr>
<tr>
<td>show lldp info remote-device</td>
<td>Shows LLDP global and interface-specific configuration settings for remote devices</td>
<td>PE</td>
</tr>
<tr>
<td>show lldp info statistics</td>
<td>Shows statistical counters for all LLDP-enabled interfaces</td>
<td>PE</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Shows summary and detailed information for LLDP neighbor devices</td>
<td>PE</td>
</tr>
</tbody>
</table>

* Vendor-specific options may or may not be advertised by neighboring devices.
lldp

This command enables LLDP globally on the switch. Use the no form to disable LLDP.

Syntax

[no] lldp

Default Setting

Enabled

Command Mode

Global Configuration

Example

Console(config)#lldp
Console(config)#

lldp holdtime-multiplier

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the no form to restore the default setting.

Syntax

lldp holdtime-multiplier value

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule:
minimum of ((Transmission Interval * Holdtime Multiplier), or 65536)
(Range: 2 - 10)

Default Setting

Holdtime multiplier: 4
TTL: 4*30 = 120 seconds

Command Mode

Global Configuration

Command Usage

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

Console(config)#lldp holdtime-multiplier 10
Console(config)#
lldp med-fast-start-count

This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. Use the no form to restore the default setting.

Syntax

```plaintext
lldp med-fast-start-count packets
no lldp med-fast-start-count

seconds - Amount of packets. (Range: 1-10 packets; Default: 4 packets)
```

Default Setting

4 packets

Command Mode

Global Configuration

Command Usage

This parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Example

```plaintext
Console(config)#lldp med-fast-start-count 6
Console(config)#
```

lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the no form to restore the default setting.

Syntax

```plaintext
lldp notification-interval seconds
no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)
```

Default Setting

5 seconds

Command Mode

Global Configuration

Command Usage

◆ This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#lldp notification-interval 30
Console(config)#
```

**lldp refresh-interval**  This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

**Syntax**

```
lldp refresh-interval seconds
no lldp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)
```

**Default Setting**

30 seconds

**Command Mode**

Global Configuration

**Example**

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

**lldp reinit-delay**  This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

**Syntax**

```
lldp reinit-delay seconds
no lldp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP.
(Range: 1 - 10 seconds)
```

**Default Setting**

2 seconds
**Command Mode**
Global Configuration

**Command Usage**
When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

**Example**
```
Console(config)#lldp reinit-delay 10
Console(config)#
```

**lldp tx-delay** This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

**Syntax**

```
lldp tx-delay seconds
no lldp tx-delay
```

- `seconds` - Specifies the transmit delay. (Range: 1 - 8192 seconds)

**Default Setting**
2 seconds

**Command Mode**
Global Configuration

**Command Usage**
- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

- This attribute must comply with the following rule:
  \(4 \times \text{tx-delay} \leq \text{refresh-interval}\)

**Example**
```
Console(config)#lldp tx-delay 10
Console(config)#
```
**lldp admin-status**  
This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

**Syntax**

```
lldp admin-status {rx-only | tx-only | tx-rx}
no lldp admin-status
```

**Default Setting**

tx-rx

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

**lldp basic-tlv management-ip-address**  
This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

**Syntax**

```
[lno] lldp basic-tlv management-ip-address
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

**Example**

```bash
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

**lldp basic-tlv port-description**

This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

**Syntax**

```
[no] lldp basic-tlv port-description
```

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

**Example**

```bash
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

**lldp basic-tlv system-capabilities**

This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

**Syntax**

```
[no] lldp basic-tlv system-capabilities
```

**Default Setting**

Enabled
**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

**lldp basic-tlv system-description**
This command configures an LLDP-enabled port to advertise the system description. Use the `no` form to disable this feature.

**Syntax**

```
[no] lldp basic-tlv system-description
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

**lldp basic-tlv system-name**
This command configures an LLDP-enabled port to advertise the system name. Use the `no` form to disable this feature.

**Syntax**

```
[no] lldp basic-tlv system-name
```

**Default Setting**
Enabled
**Chapter 22 | LLDP Commands**

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the `hostname` command.

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

**lldp dot1-tlv proto-ident**
This command configures an LLDP-enabled port to advertise the supported protocols. Use the `no` form to disable this feature.

**Syntax**

```
[no] lldp dot1-tlv proto-ident
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
This option advertises the protocols that are accessible through this interface.

**Example**

```console
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

**lldp dot1-tlv proto-vid**
This command configures an LLDP-enabled port to advertise port-based protocol VLAN information. Use the `no` form to disable this feature.

**Syntax**

```
[no] lldp dot1-tlv proto-vid
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
This option advertises the protocols that are accessible through this interface.
Command Usage
This option advertises the port-based protocol VLANs configured on this interface (see “Configuring Protocol-based VLANs” on page 525).

Example
```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

**lldp dot1-tlv pvid**
This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the no form to disable this feature.

**Syntax**
```
[no] lldp dot1-tlv pvid
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
The port’s default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the switchport native vlan command).

Example
```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

**lldp dot1-tlv vlan-name**
This command configures an LLDP-enabled port to advertise its VLAN name. Use the no form to disable this feature.

**Syntax**
```
[no] lldp dot1-tlv vlan-name
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)
**Command Usage**
This option advertises the name of all VLANs to which this interface has been assigned. See "switchport allowed vlan" on page 506 and “protocol-vlan protocol-group (Configuring Interfaces)” on page 527.

**Example**
```plaintext
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

**lldp dot3-tlv link-agg**
This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the `no` form to disable this feature.

**Syntax**
```
[no] lldp dot3-tlv link-agg
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

**Example**
```plaintext
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

**lldp dot3-tlv mac-phy**
This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the `no` form to disable this feature.

**Syntax**
```
[no] lldp dot3-tlv mac-phy
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)
**Command Usage**
This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

**Example**
```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

**Ildp dot3-tlv max-frame**
This command configures an LLDP-enabled port to advertise its maximum frame size. Use the `no` form to disable this feature.

**Syntax**
```
[no] lldp dot3-tlv max-frame
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)

**Command Usage**
Refer to "Frame Size" on page 107 for information on configuring the maximum frame size for this switch.

**Example**
```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

**Ildp dot3-tlv poe**
This command configures an LLDP-enabled port to advertise its Power-over-Ethernet (PoE) capabilities. Use the `no` form to disable this feature.

**Syntax**
```
[no] lldp dot3-tlv poe
```

**Default Setting**
Enabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)
Command Usage
This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

lldp med-location civic-addr This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the no form to restore the default settings.

Syntax

```
lldp med-location civic-addr [country country-code] [what device-type] [ca-type ca-value]
no lldp med-location civic-addr [country] [what] [ca-type]
```

- **country-code** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)
- **device-type** – The type of device to which the location applies.
  - 0 – Location of DHCP server.
  - 1 – Location of network element closest to client.
  - 2 – Location of client.
- **ca-type** – A one-octet descriptor of the data civic address value. (Range: 0-255)
- **ca-value** – Description of a location. (Range: 1-32 characters)

Default Setting
Not advertised
No description

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
- Use this command without any keywords to advertise location identification details.
- Use the ca-type to advertise the physical location of the device, that is the city, street number, building and room information. The address location is
specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 138: LLDP MED Location CA Types

<table>
<thead>
<tr>
<th>CA Type</th>
<th>Description</th>
<th>CA Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>National subdivisions (state, canton, province)</td>
<td>California</td>
</tr>
<tr>
<td>2</td>
<td>County, parish</td>
<td>Orange</td>
</tr>
<tr>
<td>3</td>
<td>City, township</td>
<td>Irvine</td>
</tr>
<tr>
<td>4</td>
<td>City division, borough, city district</td>
<td>West Irvine</td>
</tr>
<tr>
<td>5</td>
<td>Neighborhood, block</td>
<td>Riverside</td>
</tr>
<tr>
<td>6</td>
<td>Group of streets below the neighborhood level</td>
<td>Exchange</td>
</tr>
<tr>
<td>18</td>
<td>Street suffix or type</td>
<td>Avenue</td>
</tr>
<tr>
<td>19</td>
<td>House number</td>
<td>320</td>
</tr>
<tr>
<td>20</td>
<td>House number suffix</td>
<td>A</td>
</tr>
<tr>
<td>21</td>
<td>Landmark or vanity address</td>
<td>Tech Center</td>
</tr>
<tr>
<td>26</td>
<td>Unit (apartment, suite)</td>
<td>Apt 519</td>
</tr>
<tr>
<td>27</td>
<td>Floor</td>
<td>5</td>
</tr>
<tr>
<td>28</td>
<td>Room</td>
<td>509B</td>
</tr>
</tbody>
</table>

Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

- For the location options defined for device-type, normally option 2 is used to specify the location of the client device. In situations where the client device location is not known, 0 and 1 can be used, providing the client device is physically close to the DHCP server or network element.

Example

The following example enables advertising location identification details.

```console
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 5 Exchange
Console(config-if)#lldp med-location civic-addr 6 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#
```

---

- 687 -
**lldp med-notification**  
This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

**Syntax**

\[
\text{[no]} \text{ lldp med-notification}
\]

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the `lldp notification-interval` command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

◆ SNMP trap destinations are defined using the `snmp-server host` command.

◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

**lldp med-tlv ext-poe**  
This command configures an LLDP-MED-enabled port to advertise and accept Extended Power-over-Ethernet configuration and usage information. Use the **no** form to disable this feature.

**Syntax**

\[
\text{[no]} \text{ lldp med-tlv ext-poe}
\]

**Default Setting**

Enabled

**Command Mode**

Interface Configuration (Ethernet, Port Channel)
Command Usage
This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode). Note that this device does not support PoE capabilities.

Example

```bash
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv ext-poe
Console(config-if)#
```

lldp med-tlv inventory
This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

Syntax

```
[no] lldp med-tlv inventory
```

Default Setting
Enabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

Example

```bash
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#
```

lldp med-tlv location
This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

Syntax

```
[no] lldp med-tlv location
```

Default Setting
Enabled

Command Mode
Interface Configuration (Ethernet, Port Channel)
Command Usage
This option advertises location identification details.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#
```

`lldp med-tlv med-cap` This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the `no` form to disable this feature.

Syntax
```
[no] lldp med-tlv med-cap
```

Default Setting
Enabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

`lldp med-tlv network-policy` This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the `no` form to disable this feature.

Syntax
```
[no] lldp med-tlv network-policy
```

Default Setting
Enabled

Command Mode
Interface Configuration (Ethernet, Port Channel)
Command Usage
This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

lldp notification
This command enables the transmission of SNMP trap notifications about LLDP changes. Use the no form to disable LLDP notifications.

Syntax

```
[no] lldp notification
```

Default Setting
Enabled

Command Mode
Interface Configuration (Ethernet, Port Channel)

Command Usage
◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

◆ SNMP trap destinations are defined using the snmp-server host command.

◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```
show lldp config  This command shows LLDP configuration settings for all ports.

Syntax

```
show lldp config [detail interface]
```

**detail** - Shows configuration summary.

**interface**

```
ethernet unit/port
```

- *unit* - Unit identifier. (Range: 1)
- *port* - Port number. (Range: 1-28/52)

**port-channel channel-id** (Range: 1-12)

Command Mode

Privileged Exec

Example

The following example shows all basic LLDP parameters are enabled on Port 1.

```
Console#show lldp config
LLDP Global Configuration
LLDP Enabled                     : Yes
LLDP Transmit Interval           : 30 seconds
LLDP Hold Time Multiplier        : 4
LLDP Delay Interval              : 2 seconds
LLDP Re-initialization Delay    : 2 seconds
LLDP Notification Interval       : 5 seconds
LLDP MED Fast Start Count        : 4

LLDP Port Configuration
Port     Admin Status Notification Enabled
-------- ------------ --------------------
Eth 1/1   Tx-Rx        True
Eth 1/2   Tx-Rx        True
Eth 1/3   Tx-Rx        True
Eth 1/4   Tx-Rx        True
Eth 1/5   Tx-Rx        True

Console#show lldp config detail ethernet 1/1
LLDP Port Configuration Detail
Port               : Eth 1/1
Admin Status       : Tx-Rx
Notification Enabled: True
Basic TLVs Advertised: port-description
                      system-name
                      system-description
                      system-capabilities
                      management-ip-address
802.1 specific TLVs Advertised: port-vid
                                  vlan-name
                                  proto-vlan
                                  proto-ident
802.3 specific TLVs Advertised: mac-phy
                                  poe
                                  link-agg
                                  max-frame
```
show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

```
show lldp info local-device [detail interface]

detail - Shows configuration summary.

interface

ethernet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-12)
```

Command Mode

Privileged Exec

Example

```
Console#show lldp info local-device
LLDP Local Global Information
Chassis Type : MAC Address
Chassis ID : FC-0A-81-B7-C7-E0
System Name : 
System Description : EX-3524 Managed POE/POE+ Switch
System Capabilities Support : Bridge
System Capabilities Enabled : Bridge
Management Address : 192.168.0.3 (IPv4)

LLDP Local Port Information
Port Port ID Type Port ID Port Description
-------------- --------------- ------------------------------
Eth 1/1 MAC Address FC-0A-81-B7-C7-E1 Ethernet Port on unit 1, port 1
Eth 1/2 MAC Address FC-0A-81-B7-C7-E2 Ethernet Port on unit 1, port 2
Eth 1/3 MAC Address FC-0A-81-B7-C7-E3 Ethernet Port on unit 1, port 3
Eth 1/4 MAC Address 00-1A-7E-AC-2B-16 Ethernet Port on unit 1, port 4
.
.
```
show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [detail interface]

  detail - Shows detailed information.
  interface

    ethernet unit/port

    unit - Unit identifier. (Range: 1)
    port - Port number. (Range: 1-28/52)

    port-channel channel-id (Range: 1-16)

Command Mode
Privileged Exec

Example
Note that an IP phone or other end-node device which advertises LLDP-MED capabilities must be connected to the switch for information to be displayed in the “Device Class” field.

Console#show lldp info remote-device
LLDP Remote Devices Information

<table>
<thead>
<tr>
<th>Interface</th>
<th>Chassis ID</th>
<th>Port ID</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>00-1A-7E-AC-2B-12</td>
<td>00-1A-7E-AC-2B-13</td>
<td></td>
</tr>
</tbody>
</table>

Console#show lldp info remote-device detail ethernet 1/1
LLDP Remote Devices Information Detail

<table>
<thead>
<tr>
<th>Index</th>
<th>Chassis Type</th>
<th>Chassis ID</th>
<th>Port Type</th>
<th>Port ID</th>
<th>Time To Live</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>MAC Address</td>
<td>70-72-CF-91-1C-B2</td>
<td>MAC Address</td>
<td>70-72-CF-91-1C-B4</td>
<td>120 seconds</td>
<td>Ethernet Port on unit 1, port 2</td>
</tr>
</tbody>
</table>
System Description : EX-3524 Managed POE/POE+ Switch
Port Description : Ethernet Port on unit 1, port 2
System Capabilities Supported : Bridge
System Capabilities Enabled : Bridge

Management Address : 192.168.0.4 (IPv4)

Port VLAN ID : 1
Port and Protocol VLAN ID : supported, disabled
VLAN Name : VLAN 1 - DefaultVlan
Protocol Identity (Hex) : 88-CC

MAC/PHY Configuration/Status
Port Auto-neg Supported : Yes
Port Auto-neg Enabled : Yes
Port Auto-neg Advertised Cap (Hex) : 6C00
Port MAU Type : 16

Power via MDI
Power Class : PSE
Power MDI Supported : Yes
Power MDI Enabled : Yes
Power Pair Controllable : No
Power Pairs : Spare
Power Classification : Class 1

Link Aggregation
Link Aggregation Capable : Yes
Link Aggregation Enable : No
Link Aggregation Port ID : 0

Max Frame Size : 1522

Console#

**show lldp info statistics**  This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

**Syntax**

```
show lldp info statistics [detail interface]
```

- **detail** - Shows configuration summary.
- **interface**
  - **ethernet unit/port**
    - **unit** - Unit identifier. (Range: 1)
    - **port** - Port number. (Range: 1-28/52)
  - **port-channel channel-id** (Range: 1-16)

**Command Mode**
Privileged Exec
Example

```bash
switch#show lldp info statistics
LLDP Global Statistics
Neighbor Entries List Last Updated : 96 seconds
New Neighbor Entries Count : 3
Neighbor Entries Deleted Count : 1
Neighbor Entries Dropped Count : 0
Neighbor Entries Ageout Count : 0

LLDP Port Statistics
Port     NumFramesRecvd NumFramesSent NumFramesDiscarded
-------- -------------- ------------- ------------------
Eth 1/1             822           821                  0
Eth 1/2               0             0                  0
Eth 1/3               0             0                  0
Eth 1/4               0             0                  0
Eth 1/5             849           862                  0
:
```

```
switch#show lldp info statistics detail ethernet 1/1
LLDP Port Statistics Detail
Port Name : Eth 1/1
Frames Discarded : 0
Frames Invalid    : 0
Frames Received   : 824
Frames Sent       : 823
TLVs Unrecognized : 0
TLVs Discarded    : 0
Neighbor Ageouts  : 0
```

```bash
switch#
```

**show lldp neighbors**  This command shows LLDP summary and detailed information for LLDP neighbors attached to an LLDP-enabled port.

**Syntax**

```
show lldp neighbors [detail interface]

detail - Shows detailed information.

interface

eternet unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel channel-id (Range: 1-16)
```

**Command Mode**

Privileged Exec
Example

```
Console#show lldp neighbors

LLDP Neighbors Information

<table>
<thead>
<tr>
<th>Interface</th>
<th>Chassis ID</th>
<th>Port ID</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1/1</td>
<td>70-72-CF-94-22-34</td>
<td>70-72-CF-94-22-35</td>
<td></td>
</tr>
<tr>
<td>Eth 1/2</td>
<td>00-E0-0C-10-90-00</td>
<td>00-E0-0C-10-90-0B</td>
<td></td>
</tr>
</tbody>
</table>

Console#show lldp neighbors detail ethernet 1/2

LLDP Neighbors Information Detail

<table>
<thead>
<tr>
<th>Index</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis Type</td>
<td>MAC Address</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>00-E0-0C-00-00-FD</td>
</tr>
<tr>
<td>Port ID Type</td>
<td>MAC Address</td>
</tr>
<tr>
<td>Port ID</td>
<td>00-E0-0C-00-00-FE</td>
</tr>
<tr>
<td>Time To Live</td>
<td>120 seconds</td>
</tr>
<tr>
<td>Port Description</td>
<td>Ethernet Port on unit 1, port 1</td>
</tr>
<tr>
<td>System Description</td>
<td>EX-3548 Managed POE/POE+ Switch</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>Bridge</td>
</tr>
<tr>
<td>Enabled Capabilities</td>
<td>Bridge</td>
</tr>
<tr>
<td>Management Address</td>
<td>192.168.0.4 (IPv4)</td>
</tr>
<tr>
<td>Port VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>Port and Protocol VLAN ID</td>
<td>supported, disabled</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>VLAN 1 - DefaultVlan</td>
</tr>
<tr>
<td>Protocol Identity (Hex)</td>
<td>88-CC</td>
</tr>
</tbody>
</table>

MAC/PHY Configuration/Status

| Port Auto-neg Supported | Yes |
| Port Auto-neg Enabled   | Yes |
| Port Auto-neg Advertised Cap (Hex) | 6C01 |
| Port MAU Type           | 30  |

Power via MDI

| Power Class | PSE |
| Power MDI Supported | Yes |
| Power MDI Enabled | Yes |
| Power Pair Controllable | No |
| Power Pairs | Spare |
| Power Classification | Class 1 |

Link Aggregation

| Link Aggregation Capable | Yes |
| Link Aggregation Enable  | No  |
| Link Aggregation Port ID | 0   |

Max Frame Size : 1522

Console#
```
Cisco Discovery Protocol (CDP) is a proprietary protocol that discovers information about neighboring devices by passing messages across the Data Link Layer. It is used to share information about nearby network equipment. Participating devices send CDP announcements from each connected network interface to the multicast address 01-00-0C-CC-CC-CC. These packets may be received by any networking devices that support CDP. By default, CDP announcements are sent every 60 seconds. Each device that supports CDP stores the information received from other devices in a table that can be viewed using the `show cdp neighbors` command. This information is refreshed each time an announcement is received, and the holdtime for that entry is reinitialized.

The information contained in CDP announcements may include the CDP version, host name, IP address and port identifier from which the announcement was sent, device type, and other device specific information.

**Table 139: CDP Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cdp</code></td>
<td>Enables CDP globally on the switch</td>
<td>GC</td>
</tr>
<tr>
<td><code>cdp hold-time</code></td>
<td>Specifies the amount of time the receiving device should hold a CDP packet sent from this switch</td>
<td>GC</td>
</tr>
<tr>
<td><code>cdp transmit-interval</code></td>
<td>Specifies the periodic transmission interval for CDP advertisements</td>
<td>GC</td>
</tr>
<tr>
<td><code>cdp version</code></td>
<td>Specifies the CDP version to use for transmitting advertisements</td>
<td>GC</td>
</tr>
<tr>
<td><code>cdp</code></td>
<td>Enables CDP on the selected interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>clear cdp table</code></td>
<td>Clears the CDP neighbor table</td>
<td>PE</td>
</tr>
<tr>
<td><code>show cdp</code></td>
<td>Shows global CDP configuration settings</td>
<td>PE</td>
</tr>
<tr>
<td><code>show cdp interface</code></td>
<td>Shows whether or not CDP is enabled on an interface</td>
<td>PE</td>
</tr>
<tr>
<td><code>show cdp neighbors</code></td>
<td>Shows information about neighbors obtained by monitoring CDP advertisements</td>
<td>PE</td>
</tr>
</tbody>
</table>
cdp  
(Global Configuration)

This command enables CDP globally on the switch. Use the no form to disable CDP.

Syntax

[no] cdp

Default Setting
Disabled

Command Mode
Global Configuration

Example

```
Console(config)#cdp
Console(config)#
```

cdp hold-time  

This command specifies the amount of time the receiving device should hold a CDP packet sent from this switch. Use the no form to restore the default setting.

Syntax

```
cdp hold-time seconds
no cdp hold-time
```

- The hold time sent in CDP update packets.
  (Range: 10-255 seconds)

Default Setting
180 seconds

Command Mode
Global Configuration

Example

```
Console(config)#cdp hold-time 100
Console(config)#
```
**cdp transmit-interval**  This command specifies the periodic transmission interval for CDP advertisements. Use the **no** form to restore the default setting.

**Syntax**

```plaintext
   cdp transmit-interval seconds
   no cdp transmit-interval
```

```
   seconds - The interval at which the switch send CDP updates.
   (Range: 5-254 seconds)
```

**Default Setting**

60 seconds

**Command Mode**

Global Configuration

**Example**

```plaintext
   Console(config)#cdp transmit-interval 120
   Console(config)#
```

**cdp version**  This command specifies the CDP version to use for transmitting advertisements. Use the **no** form to restore the default setting.

**Syntax**

```plaintext
   cdp version {1 | 2}
   no cdp version
```

```
   1 - CDP version 1.
   2 - CDP version 2.
```

**Default Setting**

Version 2

**Command Mode**

Global Configuration

**Example**

```plaintext
   Console(config)#cdp version 1
   Console(config)#
```
**cdp** (Interface Configuration)  This command enables CDP on the selected interface. Use the **no** form to disable CDP on the selected interface.

**Syntax**

```
[no] cdp
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#cdp
Console(config-if)#
```

---

**clear cdp table**  This command clears the CDP neighbor table.

**Command Mode**
Privileged Exec

**Command Usage**
When a port link goes down, CDP will also clear the peer information for this port.

**Example**

```
Console#clear cdp table
Console#
```

---

**show cdp**  This command shows the global CDP configuration settings.

**Command Mode**
Privileged Exec

**Example**

```
Console#show cdp
CDP Global Configuration
Status : Disabled
Transmit Interval : 60 seconds
Hold Time : 180 seconds
Version : 2
Console#
```
**show cdp interface**  This command shows whether or not CDP is enabled on an interface.

**Syntax**

```
show cdp interface [interface]
```

`interface`

- `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)

**Command Mode**
Privileged Exec

**Example**

```
Console#show cdp interface
Interface Status
---------- --------
Eth 1/ 1  Disabled
Eth 1/ 2  Disabled
Eth 1/ 3  Disabled...
```

**show cdp neighbors**  This command shows information about neighbors obtained by monitoring CDP advertisements.

**Syntax**

```
show cdp neighbors [detail | [interface [detail]]]
```

`detail` - Shows detailed information about CDP neighbors.

`interface`

- `ethernet unit/port`
  - `unit` - Unit identifier. (Range: 1)
  - `port` - Port number. (Range: 1-28/52)

**Command Mode**
Privileged Exec
Example

```
Console#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Interface Version Device ID Hold Time Capability Platform Port ID
              Time Time
--------- ------- --------- ------ ---------- -------- ------------------
Eth 1/40    2 EX-3524 M   180    179 S          EX-3524  ethernet 1/11
Console#
```

In addition to the information shown in Table 140, the “SW Version” field shown in this example indicates SW Version of the CDP neighbor.

Table 140: show cdp neighbors - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Codes</td>
<td>The capabilities that define the primary function(s) of the system.</td>
</tr>
<tr>
<td>Interface</td>
<td>The local port to which a remote CDP-capable device is attached.</td>
</tr>
<tr>
<td>Version</td>
<td>The software version running on the neighbor.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The name of the neighbor device, its MAC address or the serial number.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The amount of time to hold CDP messages as advertised in CDP updates received from the neighbor.</td>
</tr>
<tr>
<td>Remain Time</td>
<td>The amount of time this switch will continue to hold a CDP advertisement before discarding it.</td>
</tr>
<tr>
<td>Capability</td>
<td>The device type of the neighbor.</td>
</tr>
<tr>
<td>Platform</td>
<td>The product number of the device.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The interface type and port number of the neighbor.</td>
</tr>
</tbody>
</table>

This example shows detailed information about CDP neighbors.
Domain Name Service Commands

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the ip name-server command and domain lookup is enabled with the ip domain-lookup command.

Table 141: Address Table Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-list</td>
<td>Defines a list of default domain names for incomplete host names</td>
<td>GC</td>
</tr>
<tr>
<td>ip domain-lookup</td>
<td>Enables DNS-based host name-to-address translation</td>
<td>GC</td>
</tr>
<tr>
<td>ip domain-name</td>
<td>Defines a default domain name for incomplete host names</td>
<td>GC</td>
</tr>
<tr>
<td>ip host</td>
<td>Creates a static IPv4 host name-to-address mapping</td>
<td>GC</td>
</tr>
<tr>
<td>ip name-server</td>
<td>Specifies the address of one or more name servers to use for host name-to-address translation</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 host</td>
<td>Creates a static IPv6 host name-to-address mapping</td>
<td>GC</td>
</tr>
<tr>
<td>clear dns cache</td>
<td>Clears all entries from the DNS cache</td>
<td>PE</td>
</tr>
<tr>
<td>clear host</td>
<td>Deletes entries from the host name-to-address table</td>
<td>PE</td>
</tr>
<tr>
<td>show dns</td>
<td>Displays the configuration for DNS services</td>
<td>PE</td>
</tr>
<tr>
<td>show dns cache</td>
<td>Displays entries in the DNS cache</td>
<td>PE</td>
</tr>
<tr>
<td>show hosts</td>
<td>Displays the static host name-to-address mapping table</td>
<td>PE</td>
</tr>
</tbody>
</table>

**ip domain-list**

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the no form to remove a name from this list.

**Syntax**

```
[no] ip domain-list name
```

*name* - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

**Default Setting**

None
Command Mode
Global Configuration

Command Usage
◆ Domain names are added to the end of the list one at a time.

◆ When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.

◆ If there is no domain list, the domain name specified with the ip domain-name command is used. If there is a domain list, the default domain name is not used.

Example
This example adds two domain names to the current list and then displays the list.

```console
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS Disabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
```

Related Commands
ip domain-name (707)

**ip domain-lookup** This command enables DNS host name-to-address translation. Use the no form to disable DNS.

Syntax

```
[no] ip domain-lookup
```

Default Setting
Disabled

Command Mode
Global Configuration

Command Usage
◆ At least one name server must be specified before DNS can be enabled.

◆ If all name servers are deleted, DNS will automatically be disabled.
Example
This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS Enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

Related Commands
ip domain-name (707)
ip name-server (708)

**ip domain-name**  This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

**Syntax**

```
  ip domain-name name
  no ip domain-name
```

**name** - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

**Default Setting**
None

**Command Mode**
Global Configuration

**Example**
```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS Disabled
Default Domain Name:
  sample.com
Domain Name List:
  Name Server List:
Console#
```
Related Commands
ip domain-list (705)
ip name-server (708)
ip domain-lookup (706)

**ip host** This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

**Syntax**

```
[no] ip host name address
```

- *name* - Name of an IPv4 host. (Range: 1-100 characters)
- *address* - Corresponding IPv4 address.

**Default Setting**
No static entries

**Command Mode**
Global Configuration

**Command Usage**
Use the **no ip host** command to clear static entries, or the **clear host** command to clear dynamic entries.

**Example**
This example maps an IPv4 address to a host name.

```
Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address            TTL   Domain
---- ---- ------- --------------------  ----- ------------------------------
       2 Address 192.168.1.55                rd5
Console#
```

**ip name-server** This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

**Syntax**

```
[no] ip name-server server-address1 [server-address2 ... server-address6]
```

- *server-address1* - IPv4 or IPv6 address of domain-name server.
- *server-address2* ... *server-address6* - IPv4 or IPv6 address of additional domain-name servers.
Default Setting
None

Command Mode
Global Configuration

Command Usage
The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example
This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS disabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

Related Commands
ip domain-name (707)
ip domain-lookup (706)

ipv6 host
This command creates a static entry in the DNS table that maps a host name to an IPv6 address. Use the no form to remove an entry.

Syntax
```
[no] ipv6 host name ipv6-address
```

- **name** - Name of an IPv6 host. (Range: 1-127 characters)
- **ipv6-address** - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting
No static entries
**Command Mode**
Global Configuration

**Example**
This example maps an IPv6 address to a host name.

```
Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address            TTL   Domain
---- ---- ------- --------------------  ----- -------------------------------
 0    2 Address 192.168.1.55                rd5
 1    2 Address 2001:DB8:1::12              rd6
Console#
```

**clear dns cache**  This command clears all entries in the DNS cache.

**Command Mode**
Privileged Exec

**Example**

```
Console#clear dns cache
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Host
------- ------- ------- --------------- ------- --------
Console#
```

**clear host**  This command deletes dynamic entries from the DNS table.

**Syntax**

```
clear host [name | *]
```

- `name` - Name of the host. (Range: 1-127 characters)
- `*` - Removes all entries.

**Default Setting**
None

**Command Mode**
Privileged Exec

**Command Usage**
Use the `clear host` command to clear dynamic entries, or the `no ip host` command to clear static entries.
Example
This example clears all dynamic entries from the DNS table.

```
Console#clear host *
Console#
```

**show dns**  This command displays the configuration of the DNS service.

**Command Mode**
Privileged Exec

**Example**
```
Console#show dns
Domain Lookup Status:
   DNS enabled
Default Domain Name:
   sample.com
Domain Name List:
   sample.com.jp
   sample.com.uk
Name Server List:
   192.168.1.55
   10.1.0.55
Console#
```

**show dns cache**  This command displays entries in the DNS cache.

**Command Mode**
Privileged Exec

**Example**
```
Console#show dns cache
No.     Flag    Type       IP Address      TTL     Host
------- ------- ------- --------------- ------- ----------------------------
  3       4 Host    209.131.36.158      115 www-real.wa1.b.yahoo.com
  4       4 CNAME   POINTER TO:3        115 www.yahoo.com
  5       4 CNAME   POINTER TO:3        115 www.wa1.b.yahoo.com
Console#
```

**Table 142: show dns cache - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>The entry number for each resource record.</td>
</tr>
<tr>
<td>Flag</td>
<td>The flag is always “4” indicating a cache entry and therefore unreliable.</td>
</tr>
<tr>
<td>Type</td>
<td>This field includes “Host” which specifies the primary name for the owner, and “CNAME” which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.</td>
</tr>
</tbody>
</table>
show hosts

This command displays the static host name-to-address mapping table.

**Command Mode**
Privileged Exec

**Example**
Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts
No.  Flag Type    IP Address            TTL   Host
---- ---- ------- --------------------  ----- -------------------------------
0    2 Address 192.168.1.55                rd5
1    2 Address 2001:DB8:1::12              rd6
3    4 Address 209.131.36.158           65   www-real.wa1.b.yahoo.com
4    4 CNAME   POINTER TO:3             65   www.yahoo.com
5    4 CNAME   POINTER TO:3             65   www.wa1.b.yahoo.com
Console#
```

**Table 142: show dns cache - display description (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address associated with this record.</td>
</tr>
<tr>
<td>TTL</td>
<td>The time to live reported by the name server.</td>
</tr>
<tr>
<td>Host</td>
<td>The host name associated with this record.</td>
</tr>
</tbody>
</table>

**Table 143: show hosts - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>The entry number for each resource record.</td>
</tr>
<tr>
<td>Flag</td>
<td>The field displays “2” for a static entry, or “4” for a dynamic entry stored in the cache.</td>
</tr>
<tr>
<td>Type</td>
<td>This field includes “Address” which specifies the primary name for the owner, and “CNAME” which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with this record.</td>
</tr>
<tr>
<td>TTL</td>
<td>The time to live reported by the name server. This field is always blank for static entries.</td>
</tr>
<tr>
<td>Host</td>
<td>The host name associated with this record.</td>
</tr>
</tbody>
</table>
DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client and relay functions. Any VLAN interface on this switch can be configured to automatically obtain an IP address through DHCP. This switch can also be configured to relay DHCP client configuration requests to a DHCP server on another network.

Table 144: DHCP Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Client</td>
<td>Allows interfaces to dynamically acquire IP address information</td>
</tr>
<tr>
<td>DHCP Relay</td>
<td>Relays DHCP requests from local hosts to a remote DHCP server</td>
</tr>
</tbody>
</table>

DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 145: DHCP Client Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP for IPv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip dhcp client class-id</td>
<td>Specifies the DHCP client identifier for an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ip dhcp restart client</td>
<td>Submits a BOOTP or DHCP client request</td>
<td>PE</td>
</tr>
<tr>
<td>DHCP for IPv6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6 dhcp client rapid-commit</td>
<td>Specifies the Rapid Commit option for DHCPv6 message exchange</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 dhcp restart client vlan</td>
<td>Submits a DHCPv6 client request</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 dhcp duid</td>
<td>Shows the DHCP Unique Identifier for this switch</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 dhcp vlan</td>
<td>Shows DHCPv6 information for specified interface</td>
<td>PE</td>
</tr>
</tbody>
</table>
DHCP for IPv4

**ip dhcp client class-id**  This command specifies the DHCP client vendor class identifier for the current interface. Use the **no** form to remove the class identifier from the DHCP packet.

**Syntax**

```
ip dhcp client class-id [text text | hex hex]
```

- **no ip dhcp client class-id**
  
  - `text` - A text string. (Range: 1-32 characters)
  - `hex` - A hexadecimal value. (Range: 1-64 characters)

**Default Setting**

Class identifier option enabled, with the name EX-3524 or EX-3548.

**Command Mode**

Interface Configuration (VLAN)

**Command Usage**

- Use this command without a keyword to restore the default setting.
- This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60, 66 and 67 statements can be added to the server daemon's configuration file.

**Table 146: Options 60, 66 and 67 Statements**

<table>
<thead>
<tr>
<th>Option</th>
<th>Keyword</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>vendor-class-identifier</td>
<td>a string indicating the vendor class identifier</td>
</tr>
<tr>
<td>66</td>
<td>tftp-server-name</td>
<td>a string indicating the tftp server name</td>
</tr>
<tr>
<td>67</td>
<td>bootfile-name</td>
<td>a string indicating the bootfile name</td>
</tr>
</tbody>
</table>

- By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a “parameter request list” asking for this information. Besides, the client request also includes a “vendor class identifier” set by the **ip dhcp client class-id** command that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.
◆ The server should reply with Option 66 attributes, including the TFTP server name and boot file name.

◆ Note that the vendor class identifier can be formatted in either text or hexadecimal using the `ip dhcp client class-id` command, but the format used by both the client and server must be the same.

### Table 147: Options 55 and 124 Statements

<table>
<thead>
<tr>
<th>Option</th>
<th>Keyword</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>dhcp-parameter-request-list</td>
<td>a list of parameters, separated by ','</td>
</tr>
<tr>
<td>124</td>
<td>vendor-class-identifier</td>
<td>a string indicating the vendor class identifier</td>
</tr>
</tbody>
</table>

#### Example

```plaintext
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

**Related Commands**

`ip dhcp restart client (715)`

**ip dhcp restart client**  This command submits a BOOTP or DHCP client request.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Command Usage**

◆ This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the `ip address` command.

◆ DHCP requires the server to reassign the client’s last address if available.

◆ If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.
Example
In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
   Address is FC-0A-81-B7-C7-E0
   Index: 1001, MTU: 1500
   Address Mode is DHCP
   IP Address: 192.168.0.4 Mask: 255.255.255.0
   Proxy ARP is disabled
   DHCP Client Vendor Class ID (text): EX-3524
   DHCP Relay Server: 0.0.0.0
Console#
```

Related Commands
ip address (724)

DHCP for IPv6

`ipv6 dhcp client rapid-commit vlan vlan-id`

This command specifies the Rapid Commit option for DHCPv6 message exchange for all DHCPv6 client requests submitted from the specified interface. Use the `no` form to disable this option.

**Syntax**

```
[no] ipv6 dhcp client rapid-commit vlan vlan-id
```

- `vlan-id` - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

**Default Setting**

Disabled

**Command Mode**

Global Configuration

**Command Usage**

- DHCPv6 clients can obtain configuration parameters from a server through a normal four-message exchange (solicit, advertise, request, reply), or through a rapid two-message exchange (solicit, reply). The rapid-commit option must be enabled on both client and server for the two-message exchange to be used.

- This command allows two-message exchange method for prefix delegation. When enabled, DCHPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.
Example

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

**ipv6 dhcp restart client vlan**

This command submits a DHCPv6 client request.

**Syntax**

```
ipv6 dhcp restart client vlan vlan-id
```

- **vlan-id**: VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Command Usage**

- This command starts the DHCPv6 client process if it is not yet running by submitting requests for configuration information through the specified interface(s). When DHCPv6 is restarted, the switch may attempt to acquire an IP address prefix through stateful address auto-configuration. If the router advertisements have the "other stateful configuration" flag set, the switch may also attempt to acquire other non-address configuration information (such as a default gateway or DNS server) when DHCPv6 is restarted.

Prior to submitting a client request to a DHCPv6 server, the switch should be configured with a link-local address using the `ipv6 address autoconfig` command. The state of the Managed Address Configuration flag (M flag) and Other Stateful Configuration flag (O flag) received in Router Advertisement messages will determine the information this switch should attempt to acquire from the DHCPv6 server as described below.

- **Both M and O flags are set to 1:**
  - DHCPv6 is used for both address and other configuration settings.
  - This combination is known as DHCPv6 stateful, in which a DHCPv6 server assigns stateful addresses to IPv6 hosts.

- **The M flag is set to 0, and the O flag is set to 1:**
  - DHCPv6 is used only for other configuration settings.
  - Neighboring routers are configured to advertise non-link-local address prefixes from which IPv6 hosts derive stateless addresses.
This combination is known as DHCPv6 stateless, in which a DHCPv6 server does not assign stateful addresses to IPv6 hosts, but does assign stateless configuration settings.

- DHCPv6 clients build a list of servers by sending a solicit message and collecting advertised message replies. These servers are then ranked based on their advertised preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.

- If the rapid commit option has been enabled on the switch using the `ipv6 dhcp client rapid-commit vlan` command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

**Example**
The following command submits a client request on VLAN 1.

```
Console#ipv6 dhcp restart client vlan 1
Console#
```

**Related Commands**
- `ipv6 address autoconfig (737)`

**show ipv6 dhcp duid** This command shows the DHCP Unique Identifier for this switch.

**Command Mode**
Privileged Exec

**Command Usage**
DHCPv6 clients and servers are identified by a DHCP Unique Identifier (DUID) included in the client identifier and server identifier options. Static or dynamic address prefixes may be assigned by a DHCPv6 server based on the client’s DUID.

**Example**
```
Console#show ipv6 dhcp duid
DHCPv6 Unique Identifier (DUID): 0001-0001-4A8158B4-00E00C0000FD
Console#
```
**show ipv6 dhcp vlan**  This command shows DHCPv6 information for the specified interface(s).

**Syntax**
```
show ipv6 dhcp vlan vlan-id
```

*vlan-id* - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

**Command Mode**
Privileged Exec

**Command Usage**
Each allocation in the DHCPv6 server is identified by a DUID and a IAID. IAID means Interface Association Identifier, and is a binding between the interface and one or more IP addresses.

**Example**
```
Console# show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode, No Rapid-Commit
IAID:                           C0000F0
List of known servers:
  Server address : FE80::250:FCFF:FEF9:A494
  DUID           : 0001-0001-48CFB0D5-F48F2A006801
  Server address : FE80::250:FCFF:FEF9:A405
  DUID           : 0001-0001-38CF5AB0-F48F2A003917
Console#
```

**DHCP Relay**

This section describes commands used to configure the switch to relay DHCP requests from local hosts to a remote DHCP server.

**Table 148: DHCP Relay Option 82 Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp relay server</td>
<td>Specifies DHCP server or relay server addresses</td>
<td>IC</td>
</tr>
<tr>
<td>ip dhcp restart relay</td>
<td>Enables DHCP relay agent</td>
<td>PE</td>
</tr>
</tbody>
</table>
**ip dhcp relay server**  This command specifies the DHCP server or relay server addresses to use. Use the `no` form to clear all addresses.

**Syntax**

```
ip dhcp relay server address1 [address2 [address3 ...]]
no ip dhcp relay server
```

*address* - IP address of DHCP server. (Range: 1-5 addresses)

**Default Setting**

None

**Command Mode**

Interface Configuration (VLAN)

**Usage Guidelines**

◆ DHCP relay service applies to DHCP client requests received on the specified VLAN.

◆ This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP client request, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client’s subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.

◆ You must specify the IP address for at least one active DHCP server. Otherwise, the switch’s DHCP relay agent will not be able to forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference.

If any of the specified DHCP server addresses are not located in the same network segment with this switch, use the `ip default-gateway` or `ipv6 default-gateway` command to specify the default router through which this switch can reach other IP subnetworks.

◆ To start DHCP relay service, enter the `ip dhcp restart relay` command.

**Example**

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 192.168.10.19
Console(config-if)#
```

**Related Commands**

`ip dhcp restart relay (721)`
**ip dhcp restart relay**  This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

**Default Setting**
Disabled

**Command Mode**
Privileged Exec

**Command Usage**
This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client’s subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

**Example**
In the following example, the device is reassigned the same address.

```
Console#ip dhcp restart relay
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
   Address is 00-00-E8-93-82-A0
   Index: 1001, MTU: 1500
   Address Mode is DHCP
   IP Address: 10.1.0.254 Mask: 255.255.255.0
   Proxy ARP is disabled
   DHCP Client Vendor Class ID (text): EX-3524
   DHCP relay server: 0.0.0.0
Console#
```

**Related Commands**

*ip dhcp relay server (720)*
IP Interface Commands

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

Table 149: IP Interface Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Interface</td>
<td>Configures an IPv4 address for the switch</td>
</tr>
<tr>
<td>IPv6 Interface</td>
<td>Configures an IPv6 address for the switch</td>
</tr>
<tr>
<td>ND Snooping</td>
<td>Maintains IPv6 prefix table and user address binding table which can be used for stateless address auto-configuration or for address filtering by IPv6 Source Guard</td>
</tr>
</tbody>
</table>

IPv4 Interface

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to establish a default gateway between this device and management stations or other devices that exist on another network segment.

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

Table 150: IPv4 Interface Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic IPv4 Configuration</td>
<td>Configures the IP address for interfaces and the gateway router</td>
</tr>
<tr>
<td>ARP Configuration</td>
<td>Configures static, dynamic and proxy ARP service</td>
</tr>
</tbody>
</table>
This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 151: Basic IP Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip address</code></td>
<td>Sets the IP address for the current interface</td>
<td>IC</td>
</tr>
<tr>
<td><code>ip default-gateway</code></td>
<td>Defines the default gateway through which this router can reach other subnetworks</td>
<td>GC</td>
</tr>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the IP settings for this device</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip route</code></td>
<td>Displays specified entries in the routing table</td>
<td>PE</td>
</tr>
<tr>
<td><code>show ip traffic</code></td>
<td>Displays statistics for IP, ICMP, UDP, TCP and ARP protocols</td>
<td>PE</td>
</tr>
<tr>
<td><code>traceroute</code></td>
<td>Shows the route packets take to the specified host</td>
<td>PE</td>
</tr>
<tr>
<td><code>ping</code></td>
<td>Sends ICMP echo request packets to another node on the network</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

**ip address**  
This command sets the IPv4 address for the currently selected VLAN interface. Use the **no** form to remove an IP address.

**Syntax**

```
ip address <ip-address netmask [secondary] [default-gateway ip-address] | bootp | dhcp>  
no ip address [ip-address netmask [secondary] | dhcp]
```

- `ip-address` - IP address
- `netmask` - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask can be either in the traditional format xxx.xxx.xxx.xxx or use classless format with the range /5 to /32. For example the subnet 255.255.224.0 would be /19.
- `secondary` - Specifies a secondary IP address.
- `default-gateway` - The default gateway. (Refer to the `ip default-gateway` command which provides the same function.)
- `bootp` - Obtains IP address from BOOTP.
- `dhcp` - Obtains IP address from DHCP.

**Default Setting**

DHCP

**Command Mode**

Interface Configuration (VLAN)
Command Usage

◆ If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router’s host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.

◆ Before any network interfaces are configured on the router, first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.

◆ An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.

◆ An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router/switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.

◆ If bootp or dhcp options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the ip dhcp restart client command to re-start broadcasting service requests, or reboot the switch.

NOTE: Each VLAN group can be assigned its own IP interface address. You can manage the switch via any of these IP addresses.
**Example**
In the following example, the device is assigned an address in VLAN 1.

```console
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

This example assigns an IP address to VLAN 2 using a classless network mask.

```console
Console(config)#interface vlan 2
Console(config-if)#ip address 10.2.2.1/24
Console(config-if)#
```

**Related Commands**
- `ip dhcp restart client (715)`
- `ip default-gateway (726)`
- `ipv6 address (736)`

**ip default-gateway**
This command specifies the default gateway for destinations not found in local routing tables. Use the **no** form to remove a default gateway.

**Syntax**
```
ip default-gateway gateway
no ip default-gateway
```

- `gateway` - IP address of the default gateway

**Default Setting**
No default gateway is established.

**Command Mode**
Global Configuration

**Command Usage**
- The default gateway can also be defined using the following Global configuration command: `ip route 0.0.0.0 0.0.0.0 gateway-address`.
- Static routes can also be defined using the `ip route` command to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address for a default gateway, include zone-id information indicating the VLAN identifier.
after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

**Example**
The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

**Related Commands**
ip address (724)  
ip route (772)  
ipv6 default-gateway (735)

**show ip interface**  This command displays the settings of an IPv4 interface.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
   Address is FC-0A-81-B7-C7-E0
   Index: 1001, MTU: 1500
   Address Mode is DHCP
   IP Address: 192.168.0.4 Mask: 255.255.255.0
   Proxy ARP is disabled
   DHCP Client Vendor Class ID (text): EX-3524
   DHCP Relay Server: 0.0.0.0
Console#
```

**Related Commands**
ip address (724)  
show ipv6 interface (745)

**show ip traffic**  This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ip traffic
IP Statistics:
   IP received 7845 total received
                  header errors
                  unknown protocols
                  address errors
```

---

Chapter 26  |  IP Interface Commands
IPv4 Interface

---
Chapter 26 | IP Interface Commands
IPv4 Interface

discards
7845 delivers
reassembly request datagrams
reassembly succeeded
reassembly failed

IP sent
forwards datagrams
9903 requests
discards
no routes
generated fragments
fragment succeeded
fragment failed

ICMP Statistics:
ICMP received
input
errors
destination unreachable messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
redirect messages
timestamp request messages
timestamp reply messages
source quench messages
address mask request messages
address mask reply messages

ICMP sent
output
errors
destination unreachable messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
redirect messages
timestamp request messages
timestamp reply messages
source quench messages
address mask request messages
address mask reply messages

UDP Statistics:
input
no port errors
other errors
output

TCP Statistics:
7841 input
input errors
9897 output

Console#

traceroute  This command shows the route packets take to the specified destination.

Syntax

traceroute host

host - IP address or alias of the host.
Default Setting
None

Command Mode
Privileged Exec

Command Usage
◆ Use the traceroute command to determine the path taken to reach a specified destination.

◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

◆ The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

◆ If the target device does not respond or other errors are detected, the switch will indicate this by one of the following messages:
  - * - No Response
  - H - Host Unreachable
  - N - Network Unreachable
  - P - Protocol Unreachable
  - O - Other

Example

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.
Traceroute to 192.168.0.1, 30 hops max, timeout is 3 seconds
Hop Packet 1 Packet 2 Packet 3 IP Address
--- -------- -------- -------- ---------------
1    20 ms   <10 ms   <10 ms 192.168.0.1
Trace completed.
Console#
```
**ping**  This command sends (IPv4) ICMP echo request packets to another node on the network.

**Syntax**

```
ping host [count count] [size size]
```

- **host** - IP address or alias of the host.
- **count** - Number of packets to send. (Range: 1-16)
- **size** - Number of bytes in a packet. (Range: 32-512)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

**Default Setting**

- count: 5
- size: 32 bytes

**Command Mode**

Normal Exec, Privileged Exec

**Command Usage**

- Use the **ping** command to see if another site on the network can be reached.

- The following are some results of the **ping** command:
  
  - **Normal response** - The normal response occurs in one to ten seconds, depending on network traffic.
  
  - **Destination does not respond** - If the host does not respond, a “timeout” appears in ten seconds.
  
  - **Destination unreachable** - The gateway for this destination indicates that the destination is unreachable.
  
  - **Network or host unreachable** - The gateway found no corresponding entry in the route table.

- When pinging a host name, be sure the DNS server has been defined (page 708) and host name-to-address translation enabled (page 706). If necessary, local devices can also be specified in the DNS static host table (page 708).

**Example**

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 3 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
```
Ping statistics for 10.1.0.9:
5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms

Related Commands
interface (378)

ARP Configuration
This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 152: Address Resolution Protocol Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Adds a static entry in the ARP cache</td>
<td>GC</td>
</tr>
<tr>
<td>ip proxy-arp</td>
<td>Enables proxy ARP service</td>
<td>IC</td>
</tr>
<tr>
<td>clear arp-cache</td>
<td>Deletes all dynamic entries from the ARP cache</td>
<td>PE</td>
</tr>
<tr>
<td>show arp</td>
<td>Displays entries in the ARP cache</td>
<td>NE, PE</td>
</tr>
</tbody>
</table>

arp
This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the no form to remove an entry from the cache.

Syntax

\[
\text{arp ip-address hardware-address} \\
\text{no arp ip-address}
\]

ip-address - IP address to map to a specified hardware address.

hardware-address - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting
No default entries

Command Mode
Global Configuration

Command Usage

◆ The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.

◆ The maximum number of static entries allowed in the ARP cache is 32.
You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

Static entries will not be aged out nor deleted when power is reset. A static entry can only be removed through the configuration interface.

Example

```console
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

- clear arp-cache (733)
- show arp (733)

**ip proxy-arp** This command enables proxy Address Resolution Protocol (ARP). Use the `no` form to disable proxy ARP.

**Syntax**

```
[no] ip proxy-arp
```

**Default Setting**

Disabled

**Command Mode**

Interface Configuration (VLAN)

**Command Usage**

- Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.

- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

**Example**

```console
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```
clear arp-cache  This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

**Command Mode**
Privileged Exec

**Example**
This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Do you want to continue this operation (y/n)? y
Console#
```

show arp  This command displays entries in the Address Resolution Protocol (ARP) cache.

**Command Mode**
Normal Exec, Privileged Exec

**Command Usage**
This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type “other” indicates local addresses for this router.

**Example**
This example displays all entries in the ARP cache.

```
Console#show arp
ARP Cache Timeout: 1200 (seconds)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.0</td>
<td>FF-FF-FF-FF-FF-FF other</td>
<td>VLAN1</td>
<td></td>
</tr>
<tr>
<td>10.1.0.254</td>
<td>00-00-AB-CD-00-00 other</td>
<td>VLAN1</td>
<td></td>
</tr>
<tr>
<td>10.1.0.255</td>
<td>FF-FF-FF-FF-FF-FF other</td>
<td>VLAN1</td>
<td></td>
</tr>
<tr>
<td>145.30.20.23</td>
<td>09-50-40-30-20-10 dynamic</td>
<td>VLAN3</td>
<td></td>
</tr>
</tbody>
</table>

Total entry : 5
Console#
```
**IPv6 Interface**

This switch supports the following IPv6 interface commands.

### Table 153: IPv6 Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface Address Configuration and Utilities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6 default-gateway</td>
<td>Sets an IPv6 default gateway for traffic with no known next hop</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>Configures an IPv6 global unicast address, and enables IPv6 on an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 address autoconfig</td>
<td>Enables automatic configuration of IPv6 global unicast addresses on an interface and enables IPv6 on the interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 address eui-64</td>
<td>Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 address link-local</td>
<td>Configures an IPv6 link-local address for an interface and enables IPv6 on the interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>Enables IPv6 on an interface that has not been configured with an explicit IPv6 address</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 mtu</td>
<td>Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface</td>
<td>IC</td>
</tr>
<tr>
<td>show ipv6 default-gateway</td>
<td>Displays the current IPv6 default gateway</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability and configured settings for IPv6 interfaces</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 mtu</td>
<td>Displays maximum transmission unit (MTU) information for IPv6 interfaces</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 traffic</td>
<td>Displays statistics about IPv6 traffic</td>
<td>PE</td>
</tr>
<tr>
<td>clear ipv6 traffic</td>
<td>Resets IPv6 traffic counters</td>
<td>PE</td>
</tr>
<tr>
<td>ping6</td>
<td>Sends IPv6 ICMP echo request packets to another node on the network</td>
<td>PE</td>
</tr>
<tr>
<td>traceroute6</td>
<td>Shows the route packets take to the specified host</td>
<td>PE</td>
</tr>
<tr>
<td><strong>Neighbor Discovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6 nd dad attempts</td>
<td>Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd ns-interval</td>
<td>Configures the interval between IPv6 neighbor solicitation retransmissions on an interface</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd raguard</td>
<td>Blocks incoming Router Advertisement and Router Redirect packets</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd reachable-time</td>
<td>Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred</td>
<td>IC</td>
</tr>
<tr>
<td>clear ipv6 neighbors</td>
<td>Deletes all dynamic entries in the IPv6 neighbor discovery cache</td>
<td>PE</td>
</tr>
</tbody>
</table>
Interface Address Configuration and Utilities

**ipv6 default-gateway**

This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the `no` form to remove a previously configured default gateway.

**Syntax**

```
ipv6 default-gateway ipv6-address
no ipv6 address
```

- `ipv6-address` - The IPv6 address of the default next hop router to use for destinations with no known next hop.

**Default Setting**

No default gateway is defined

**Command Mode**

Global Configuration

**Command Usage**

- All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

- An IPv6 default gateway must be defined if the destination has been assigned an IPv6 address and is located in a different IP segment.

- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

**Example**

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1
Console(config)#
```
Related Commands
show ipv6 default-gateway (744)
ip default-gateway (726)

**ipv6 address**  
This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

**Syntax**

```
[no] ipv6 address ipv6-address[/prefix-length]
```

- *ipv6-address* - A full IPv6 address including the network prefix and host address bits.
- *prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

**Default Setting**
No IPv6 addresses are defined

**Command Mode**
Interface Configuration (VLAN)

**Command Usage**
- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command, or it can be automatically configured using the `ipv6 address autoconfig` command.

- If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch’s MAC address in modified EUI-64 format.)

- If a duplicate address is detected, a warning message is sent to the console.
Example
This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
fe80::250:fcff:fef9:a494%1/64
Global unicast address(es):
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
 ff02::1:ff00:72
 ff02::1:ff9:a494
 ff02::1
 IPv6 link MTU is 1500 bytes
 ND DAD is enabled, number of DAD attempts: 3.
 ND retransmit interval is 1000 milliseconds
 ND advertised retransmit interval is 0 milliseconds
 ND reachable time is 30000 milliseconds
 ND advertised reachable time is 0 milliseconds
 ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands
ipv6 address eui-64 (739)
ipv6 address autoconfig (737)
show ipv6 interface (745)
ip address (724)

**ipv6 address autoconfig**
This command enables stateless autoconfiguration of IPv6 addresses on an
interface and enables IPv6 on the interface. The network portion of the address is
based on prefixes received in IPv6 router advertisement messages; the host portion
is based on the modified EUI-64 form of the interface identifier (i.e., the switch's
MAC address). Use the **no** form to remove the address generated by this command.

**Syntax**
```
[no] ipv6 address autoconfig
```

**Default Setting**
No IPv6 addresses are defined

**Command Mode**
Interface Configuration (VLAN)

**Command Usage**
◆ If a link local address has not yet been assigned to this interface, this command
will dynamically generate a global unicast address (if a global prefix is included
in received router advertisements) and a link local address for the interface.
(The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.

◆ If a duplicate address is detected, a warning message is sent to the console.

◆ When DHCPv6 is restarted, the switch may attempt to acquire an IP address prefix through stateful address autoconfiguration. If the router advertisements have the "other stateful configuration" flag set, the switch may also attempt to acquire other non-address configuration information (such as a default gateway) from a DHCPv6 server when DHCPv6 is restarted.

Example
This example assigns a dynamic global unicast address to the switch.

```console
Console(config)#interface vlan 1
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale, AUTOCONFIG is enabled
Link-Local Address:
  FE80::2E0:CFF:FE00:FD/64
Global Unicast Address(es):
    valid lifetime -1 preferred lifetime -1
Joined Group Address(es):
  FF02::1:FF00:1000
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands
- ipv6 address (736)
- show ipv6 interface (745)
**ipv6 address eui-64**

This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

**Syntax**

```
ipv6 address ipv6-prefix/prefix-length eui-64

no ipv6 address [ipv6-prefix/prefix-length eui-64]
```

- `ipv6-prefix` - The IPv6 network portion of the address assigned to the interface.
- `prefix-length` - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

**Default Setting**

No IPv6 addresses are defined

**Command Mode**

Interface Configuration (VLAN)

**Command Usage**

- The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)

- Note that the value specified in the `ipv6-prefix` may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.

- If a duplicate address is detected, a warning message is sent to the console.

- IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

- For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for
globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

◆ This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

Example
This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
   fe80::250:fcff:fef9:a494%1/64
Global unicast address(es):
   2001:db8:0:1:fe0a:81ff:feb7:c7e0/64, subnet is 2001:db8:0:1::/64[EUI]
   2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
   ff02::1:ffb7:c7e0
   ff02::1:ff00:72
   ff02::1:fff9:a494
   ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

Related Commands
ipv6 address autoconfig (737)
show ipv6 interface (745)
ipv6 address link-local  This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the no form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the no form with a specific address to remove it from the interface.

Syntax

```
ipv6 address ipv6-address link-local

no ipv6 address [ipv6-address link-local]
```

- ipv6-address - The IPv6 address assigned to the interface.

Default Setting
No IPv6 addresses are defined

Command Mode
Interface Configuration (VLAN)

Command Usage
- The specified address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be in the range of FE80~FEBF.

- The address specified with this command replaces a link-local address that was automatically generated for the interface.

- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.

- If a duplicate address is detected, a warning message is sent to the console.

Example
This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that a prefix in the range of FE80~FEBF is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
```

```
(Console)#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
  fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
  2001:db8:0:1:fe0a:81ff:feb7:c7e0/64, subnet is 2001:db8:0:1::/64(EUI)
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
  ff02::1:ff19:6779
  ff02::1:ff7:c7e0
  ff02::1:ff00:72
```
IP Interface Commands
IPv6 Interface

 ff02::1
 IPv6 link MTU is 1500 bytes
 ND DAD is enabled, number of DAD attempts: 3.
 ND retransmit interval is 1000 milliseconds
 ND advertised retransmit interval is 0 milliseconds
 ND reachable time is 30000 milliseconds
 ND advertised reachable time is 0 milliseconds
 ND advertised router lifetime is 1800 seconds

 Console#

 Related Commands
 ipv6 enable (742)
 show ipv6 interface (745)

 ipv6 enable

 This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

 Syntax

 `[no] ipv6 enable`

 Default Setting
 IPv6 is disabled

 Command Mode
 Interface Configuration (VLAN)

 Command Usage

 - This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the switch's MAC address to modified EUI-64 format (see page 739). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

 - If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.

 - The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

 Example

 In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

 Console(config)#interface vlan 1
 Console(config-if)#ipv6 enable
 Console(config-if)#end
 Console#show ipv6 interface
 VLAN 1 is up
IPv6 is enabled.

Link-local address:
fe80::269:3ef9:fe19:6779%1/64

Global unicast address(es):
   2001:db8:0:1:fe0a:81ff:feb7:c7e0/64, subnet is 2001:db8:0:1::/64 [EUI]
   2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96

Joined group address(es):
   ff02::1:ff19:6779
   ff02::1:ffb7:c7e0
   ff02::1:ff00:72
   ff02::1

IPv6 link MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#

Related Commands
ipv6 address link-local (741)
show ipv6 interface (745)

**ipv6 mtu**

This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the no form to restore the default setting.

**Syntax**

```
ipv6 mtu size
no ipv6 mtu
```

```
size - Specifies the MTU size. (Range: 1280-65535 bytes)
```

**Default Setting**

1500 bytes

**Command Mode**

Interface Configuration (VLAN)

**Command Usage**

◆ If a non-default value is configured, an MTU option is included in the router advertisements sent from this device.

◆ The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.

◆ IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
◆ All devices on the same physical medium must use the same MTU in order to operate correctly.

◆ IPv6 must be enabled on an interface before the MTU can be set.

**Example**
The following example sets the MTU for VLAN 1 to 1280 bytes:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

**Related Commands**
- `show ipv6 mtu (747)`
- `jumbo frame (107)`

**show ipv6 default-gateway**

This command displays the current IPv6 default gateway.

**Command Mode**
Normal Exec, Privileged Exec

**Example**
The following shows the default gateway configured for this device:

```
Console#show ipv6 default-gateway
IPv6 default gateway 2001:DB8:2222:7272::254

Console#
```
show ipv6 interface | This command displays the usability and configured settings for IPv6 interfaces.

Syntax

show ipv6 interface [brief [vlan vlan-id [ipv6-prefix/prefix-length]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

vlan-id - VLAN ID (Range: 1-4094)

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Command Mode

Exec

Example

This example displays all the IPv6 addresses configured for the switch.

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
   fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
   2001:db8:0:1:fe0a:81ff:feb7:c7e0/64, subnet is 2001:db8:0:1::/64[EUI]
   2001:db8:2222:7272::72/96, subnet is 2001:db8:2222::/96
Joined group address(es):
   ff02::1:ff19:6779
   ff02::1:ffb7:c7e0
   ff02::1:ff00:72
   ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```
This example displays a brief summary of IPv6 addresses configured on the switch.

```
Console# show ipv6 interface brief
Interface VLAN IPv6 IP Address
---------- --------- ---------- ------------------------------------
VLAN 1    Up        Up  2001:DB8:2222:7273::72/96
VLAN 1    Up        Up  FE80::2E0:CFF:FE00:FD%1/64
Console#
```
Related Commands

show ip interface (727)

**show ipv6 mtu**  
This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

**Command Mode**
Normal Exec, Privileged Exec

**Example**

The following example shows the MTU cache for this device:

```
Console#show ipv6 mtu
MTU     Since     Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
Console#
```

**Table 155: show ipv6 mtu - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.</td>
</tr>
<tr>
<td>Since</td>
<td>Time since an ICMP packet-too-big message was received from this destination.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Address which sent an ICMP packet-too-big message.</td>
</tr>
</tbody>
</table>

* No information is displayed if an IPv6 address has not been assigned to the switch.

**show ipv6 traffic**  
This command displays statistics about IPv6 traffic passing through this switch.

**Command Mode**
Privileged Exec

**Example**

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
    26 total received
    header errors
    too big errors
    no routes
    address errors
    unknown protocols
```
truncated packets
discards
26 delivers
reassembly request datagrams
reassembly succeeded
reassembly failed
IPv6 sent
forwards datagrams
133 requests
discards
no routes
generated fragments
fragment succeeded
fragment failed
ICMPv6 Statistics:
ICMPv6 received
26 input
errors
26 destination unreachable messages
packet too big messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
router solicit messages
router advertisement messages
neighbor solicit messages
neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages
ICMPv6 sent
133 output
26 destination unreachable messages
packet too big messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
3 router solicit messages
router advertisement messages
104 neighbor solicit messages
neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages
UDP Statistics:
input
no port errors
other errors
output
Console#
### Table 156: show ipv6 traffic - display description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv6 Statistics</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IPv6 received</strong></td>
<td></td>
</tr>
<tr>
<td>total received</td>
<td>The total number of input datagrams received by the interface, including those received in error.</td>
</tr>
<tr>
<td>header errors</td>
<td>The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.</td>
</tr>
<tr>
<td>too big errors</td>
<td>The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.</td>
</tr>
<tr>
<td>no routes</td>
<td>The number of input datagrams discarded because no route could be found to transmit them to their destination.</td>
</tr>
<tr>
<td>address errors</td>
<td>The number of input datagrams discarded because the IPv6 address in their IPv6 header’s destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.</td>
</tr>
<tr>
<td>unknown protocols</td>
<td>The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.</td>
</tr>
<tr>
<td>truncated packets</td>
<td>The number of input datagrams discarded because datagram frame didn’t carry enough data.</td>
</tr>
<tr>
<td>discards</td>
<td>The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.</td>
</tr>
<tr>
<td>delivers</td>
<td>The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.</td>
</tr>
<tr>
<td>reassembly request</td>
<td></td>
</tr>
<tr>
<td>datagrams</td>
<td>The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.</td>
</tr>
<tr>
<td>reassembly succeeded</td>
<td>The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.</td>
</tr>
<tr>
<td>reassembly failed</td>
<td>The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.</td>
</tr>
</tbody>
</table>
Table 156: show ipv6 traffic - display description (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv6 sent</strong></td>
<td>The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.</td>
</tr>
<tr>
<td>forwards datagrams</td>
<td>The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.</td>
</tr>
<tr>
<td>discards</td>
<td>The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.</td>
</tr>
<tr>
<td>no routes</td>
<td>The number of input datagrams discarded because no route could be found to transmit them to their destination.</td>
</tr>
<tr>
<td>generated fragments</td>
<td>The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.</td>
</tr>
<tr>
<td>fragment succeeded</td>
<td>The number of IPv6 datagrams that have been successfully fragmented at this output interface.</td>
</tr>
<tr>
<td>fragment failed</td>
<td>The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.</td>
</tr>
<tr>
<td><strong>ICMPv6 Statistics</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ICMPv6 received</strong></td>
<td></td>
</tr>
<tr>
<td>input</td>
<td>The total number of ICMP messages received by the interface which includes all those counted by ipv6IfCmplnErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.</td>
</tr>
<tr>
<td>errors</td>
<td>The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).</td>
</tr>
<tr>
<td>destination unreachable messages</td>
<td>The number of ICMP Destination Unreachable messages received by the interface.</td>
</tr>
<tr>
<td>packet too big messages</td>
<td>The number of ICMP Packet Too Big messages received by the interface.</td>
</tr>
<tr>
<td>time exceeded messages</td>
<td>The number of ICMP Time Exceeded messages received by the interface.</td>
</tr>
<tr>
<td>parameter problem</td>
<td>The number of ICMP Parameter Problem messages received by the interface.</td>
</tr>
<tr>
<td>message</td>
<td></td>
</tr>
<tr>
<td>echo request messages</td>
<td>The number of ICMP Echo (request) messages received by the interface.</td>
</tr>
<tr>
<td>echo reply messages</td>
<td>The number of ICMP Echo Reply messages received by the interface.</td>
</tr>
<tr>
<td>router solicit messages</td>
<td>The number of ICMP Router Solicit messages received by the interface.</td>
</tr>
<tr>
<td>router advertisement</td>
<td>The number of ICMP Router Advertisement messages received by the interface.</td>
</tr>
</tbody>
</table>
Table 156: show ipv6 traffic - display description (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor solicit messages</td>
<td>The number of ICMP Neighbor Solicit messages received by the interface.</td>
</tr>
<tr>
<td>neighbor advertisement messages</td>
<td>The number of ICMP Neighbor Advertisement messages received by the interface.</td>
</tr>
<tr>
<td>redirect messages</td>
<td>The number of Redirect messages received by the interface.</td>
</tr>
<tr>
<td>group membership query messages</td>
<td>The number of ICMPv6 Group Membership Query messages received by the interface.</td>
</tr>
<tr>
<td>group membership response messages</td>
<td>The number of ICMPv6 Group Membership Response messages received by the interface.</td>
</tr>
<tr>
<td>group membership reduction messages</td>
<td>The number of ICMPv6 Group Membership Reduction messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 sent</td>
<td>The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.</td>
</tr>
<tr>
<td>destination unreachable messages</td>
<td>The number of ICMP Destination Unreachable messages sent by the interface.</td>
</tr>
<tr>
<td>packet too big messages</td>
<td>The number of ICMP Packet Too Big messages sent by the interface.</td>
</tr>
<tr>
<td>time exceeded messages</td>
<td>The number of ICMP Time Exceeded messages sent by the interface.</td>
</tr>
<tr>
<td>parameter problem message</td>
<td>The number of ICMP Parameter Problem messages sent by the interface.</td>
</tr>
<tr>
<td>echo request messages</td>
<td>The number of ICMP Echo (request) messages sent by the interface.</td>
</tr>
<tr>
<td>echo reply messages</td>
<td>The number of ICMP Echo Reply messages sent by the interface.</td>
</tr>
<tr>
<td>router solicit messages</td>
<td>The number of ICMP Router Solicitation messages sent by the interface.</td>
</tr>
<tr>
<td>router advertisement messages</td>
<td>The number of ICMP Router Advertisement messages sent by the interface.</td>
</tr>
<tr>
<td>neighbor solicit messages</td>
<td>The number of ICMP Neighbor Solicit messages sent by the interface.</td>
</tr>
<tr>
<td>neighbor advertisement messages</td>
<td>The number of ICMP Router Advertisement messages sent by the interface.</td>
</tr>
<tr>
<td>redirect messages</td>
<td>The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.</td>
</tr>
<tr>
<td>group membership query messages</td>
<td>The number of ICMPv6 Group Membership Query messages sent by the interface.</td>
</tr>
<tr>
<td>group membership response messages</td>
<td>The number of ICMPv6 Group Membership Response messages sent.</td>
</tr>
<tr>
<td>group membership reduction messages</td>
<td>The number of ICMPv6 Group Membership Reduction messages sent.</td>
</tr>
<tr>
<td>UDP Statistics</td>
<td>The total number of UDP datagrams delivered to UDP users.</td>
</tr>
<tr>
<td>input</td>
<td>The total number of received UDP datagrams for which there was no application at the destination port.</td>
</tr>
</tbody>
</table>
This command shows the route packets take to the specified destination.

**Syntax**

```
traceroute6 (ipv6-address | host-name) [max-failures failure-count]
```

- `ipv6-address` - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- `host-name` - A host name string which can be resolved into an IPv6 address through a domain name server.
- `failure-count` - The maximum number of failures before which the trace route is terminated. (Range: 1-255)

**Default Setting**

Maximum failures: 5

**Command Mode**

Privileged Exec

**Command Usage**

- Use the `traceroute6` command to determine the path taken to reach a specified destination.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the `%` delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

- The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function...
prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

Example

```
Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1
Press "ESC" to abort.
Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3 seconds, 5 max failure(s) before termination.
Hop Packet 1 Packet 2 Packet 3 IPv6 Address
--- -------- -------- -------- --------------------------------------------
1 <10 ms <10 ms <10 ms FE80::2E0:CFF:FE9C:CA10%1/64
Trace completed.
Console#
```

clear ipv6 traffic This command resets IPv6 traffic counters.

**Command Mode**
Privileged Exec

**Command Usage**
This command resets all of the counters displayed by the **show ipv6 traffic** command.

Example

```
Console#clear ipv6 traffic
Console#
```

ping6 This command sends (IPv6) ICMP echo request packets to another node on the network.

**Syntax**

```
ping6 [ipv6-address | host-name] [count count] [size size]
```

- **ipv6-address** - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- **host-name** - A host name string which can be resolved into an IPv6 address through a domain name server.

- **count** - Number of packets to send. (Range: 1-16)
size - Number of bytes in a packet. (Range: 0-1500 bytes)
The actual packet size will be eight bytes larger than the size specified
because the router adds header information.

Default Setting
count: 5
size: 0 bytes

Command Mode
Privileged Exec

Command Usage
◆ Use the ping6 command to see if another site on the network can be reached,
or to evaluate delays over the path.

◆ The same link-local address may be used by different interfaces/nodes in
different zones (RFC 4007). Therefore, when specifying a link-local address,
include zone-id information indicating the VLAN identifier after the % delimiter.
For example, FE80::7272%1 identifies VLAN 1 as the interface from which the
ping is sent.

◆ When pinging a host name, be sure the DNS server has been enabled (see
page 706). If necessary, local devices can also be specified in the DNS static host
table (see page 708).

◆ When using ping6 with a host name, the switch first attempts to resolve the
alias into an IPv6 address before trying to resolve it into an IPv4 address.

Example

```
Console#ping6 FE80::2E0:CF:FE00:PC%1
Type "ESC" to abort.
PING to FE80::2E0:CF:FE00:PC%1, by 5 32-byte payload ICMP packets, timeout
is 3 seconds
response time: 20 ms  [FE80::2E0:CF:FE00:PC] seq_no: 1
response time: 0 ms  [FE80::2E0:CF:FE00:PC] seq_no: 2
response time: 0 ms  [FE80::2E0:CF:FE00:PC] seq_no: 3
response time: 0 ms  [FE80::2E0:CF:FE00:PC] seq_no: 4
response time: 0 ms  [FE80::2E0:CF:FE00:PC] seq_no: 5
Ping statistics for FE80::2E0:CF:FE00:PC%1/64:
5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
```

Console#
Neighbor Discovery

**ipv6 nd dad attempts**  
This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

**Syntax**

```
ipv6 nd dad attempts count
no ipv6 nd dad attempts
```

- **count** - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

**Default Setting**

3

**Command Mode**

Interface Configuration (VLAN)

**Command Usage**

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended (see the **vlan** command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.
Example
The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The show ipv6 interface command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
(None)
Global unicast address(es):
(None)
Joined group address(es):
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands
ipv6 nd ns-interval (756)
show ipv6 neighbors (760)

**ipv6 nd ns-interval** This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

**Syntax**

```
ipv6 nd ns-interval milliseconds
no ipv6 nd ns-interval
```

- **milliseconds** - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

**Default Setting**

1000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

**Command Mode**

Interface Configuration (VLAN)

**Command Usage**

- When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.
This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

Setting the neighbor solicitation interval to 0 means that the configured time is unspecified by this router.

**Example**
The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```plaintext
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
```

```
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  fe80::fe0a:81ff:feb7:c7e0%1/64
Global unicast address(es):
  (None)
Joined group address(es):
  ff02::1:ffb7:c7e0
  ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 3000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

**Related Commands**
`show running-config (101)`

**ipv6 nd raguard** This command blocks incoming Router Advertisement and Router Redirect packets. Use the no form to disable this feature.

**Syntax**
```
[no] ipv6 nd raguard
```

**Default Setting**
Disabled

**Command Mode**
Interface Configuration (Ethernet, Port Channel)
Command Usage

◆ IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, unintended mis-configurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.

◆ This command can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 nd raguard
Console(config-if)#
```

**ipv6 nd reachable-time**

This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

Syntax

```
ipv6 nd reachable-time milliseconds
no ipv6 nd reachable-time
```

- The time that a node can be considered reachable after receiving confirmation of reachability. (Range: 0-3600000)

Default Setting

30000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

Command Mode

Interface Configuration (VLAN)

Command Usage

◆ The time limit configured by this parameter allows the router to detect unavailable neighbors. During the neighbor discover process, an IPv6 node will multicast neighbor solicitation messages to search for neighbor nodes. For a neighbor node to be considered reachable, it must respond to the neighbor soliciting node with a neighbor advertisement message to become a confirmed neighbor, after which the reachable timer will be considered in effect for subsequent unicast IPv6 layer communications.

◆ This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.
◆ Setting the time limit to 0 means that the configured time is unspecified by this router.

**Example**
The following sets the reachable time for a remote node to 1000 milliseconds:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd reachable-time 1000
Console(config-if)#
```

clear ipv6 neighbors
This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

**Command Mode**
Privileged Exec

**Example**
The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

show ipv6 nd raguard
This command displays the configuration setting for RA Guard.

**Syntax**
```
show ipv6 nd raguard [interface]
```

- **interface**
  - **ethernet unit/port**
    - **unit** - Unit identifier. (Range: Always 1)
    - **port** - Port number. (Range: 1-28/52)
  - **port-channel channel-id** (Range: 1-16)

**Command Mode**
Privileged Exec

**Example**
```
Console#show ipv6 nd raguard interface ethernet 1/1
Interface RA Guard
--------- --------
Eth 1/ 1  Yes
Console#
```
**show ipv6 neighbors**  This command displays information in the IPv6 neighbor discovery cache.

**Syntax**

```plaintext
show ipv6 neighbors [vlan vlan-id | ipv6-address]
```

- `vlan-id` - VLAN ID (Range: 1-4094)
- `ipv6-address` - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

**Default Setting**

All IPv6 neighbor discovery cache entries are displayed.

**Command Mode**

Privileged Exec

**Example**

The following shows all known IPv6 neighbors for this switch:

```plaintext
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay, P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                            Age  Link-layer Addr   State Interface
--------------------------------------- ---- ----------------- ----- ---------
2009:db9:2229::80                         15 00-E0-0C-00-00-FD R     VLAN 1
fe80::2e0:cff:fe00:fd                      0 00-E0-0C-00-00-FD R     VLAN 1
Console#
```

**Table 157: show ipv6 neighbors - display description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of neighbor</td>
</tr>
<tr>
<td>Age</td>
<td>The time since the address was verified as reachable (in seconds). A static entry is indicated by the value “Permanent.”</td>
</tr>
<tr>
<td>Link-layer Addr</td>
<td>Physical layer MAC address.</td>
</tr>
</tbody>
</table>
ND Snooping

Neighbor Discover (ND) Snooping maintains an IPv6 prefix table and user address binding table. These tables can be used for stateless address auto-configuration or for address filtering by IPv6 Source Guard.

ND snooping maintains a binding table in the process of neighbor discovery. When it receives an Neighbor Solicitation (NS) packet from a host, it creates a new binding. If it subsequently receives a Neighbor Advertisement (NA) packet, this means that the address is already being used by another host, and the binding is therefore deleted. If it does not receive an NA packet after a timeout period, the binding will be bound to the original host. ND snooping can also maintain a prefix table used for stateless address auto-configuration by monitoring Router Advertisement (RA) packets sent from neighboring routers.
ND snooping can also detect if an IPv6 address binding is no longer valid. When a binding has been timed out, it checks to see if the host still exists by sending an NS packet to the target host. If it receives an NA packet in response, it knows that the target still exists and updates the lifetime of the binding; otherwise, it deletes the binding.

This section describes commands used to configure ND Snooping.

### Table 158: ND Snooping Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd snooping</td>
<td>Enables ND snooping globally or on a specified VLAN or range of VLANs</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd snooping auto-detect</td>
<td>Enables automatic validation of binding table entries by periodically sending NS messages and awaiting NA replies</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd snooping auto-detect retransmit count</td>
<td>Sets the number of times to send an NS message to determine if a binding is still valid</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd snooping auto-detect retransmit interval</td>
<td>Sets the interval between sending NS messages to determine if a binding is still valid</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd snooping prefix timeout</td>
<td>Sets the time to wait for an RA message before deleting an entry in the prefix table</td>
<td>GC</td>
</tr>
<tr>
<td>ipv6 nd snooping max-binding</td>
<td>Sets the maximum number of address entries which can be bound to a port</td>
<td>IC</td>
</tr>
<tr>
<td>ipv6 nd snooping trust</td>
<td>Configures a port as a trusted interface from which prefix information in RA messages can be added to the prefix table, or NS messages can be forwarded without validation</td>
<td>IC</td>
</tr>
<tr>
<td>clear ipv6 nd snooping binding</td>
<td>Clears all entries in the address binding table</td>
<td>PE</td>
</tr>
<tr>
<td>clear ipv6 nd snooping prefix</td>
<td>Clears all entries in the prefix table</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 nd snooping</td>
<td>Shows configuration settings for ND snooping</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 nd snooping binding</td>
<td>Shows entries in the binding table</td>
<td>PE</td>
</tr>
<tr>
<td>show ipv6 nd snooping prefix</td>
<td>Show entries in the prefix table</td>
<td>PE</td>
</tr>
</tbody>
</table>

**ipv6 nd snooping**

This command enables ND snooping globally or on a specified VLAN or range of VLANs. Use the **no** form to disable this feature.

**Syntax**

```
[no] ipv6 nd snooping [vlan vlan-id | vlan-range]
```

- **vlan-id** - VLAN ID. (Range: 1-4094)
- **vlan-range** - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

**Default Setting**

Disabled
Command Mode
Global Configuration

Command Usage
◆ Use this command without any keywords to enable ND snooping globally on
the switch. Use the VLAN keyword to enable ND snooping on a specific VLAN or
a range of VLANs.

◆ Once ND snooping is enabled both globally and on the required VLANs, the
switch will start monitoring RA messages to build an address prefix table as
described below:
  ▪ If an RA message is received on an untrusted interface, it is dropped. If
      received on a trusted interface, the switch adds an entry in the prefix table
      according to the Prefix Information option in the RA message. The prefix
      table records prefix, prefix length, valid lifetime, as well as the VLAN and
      port interface which received the message.
  ▪ If an RA message is not received updating a table entry with the same
      prefix for a specified timeout period, the entry is deleted.

◆ Once ND snooping is enabled both globally and on the required VLANs, the
switch will start monitoring NS messages to build a dynamic user binding table
for use in Duplicate Address Detection (DAD) or for use by other security
filtering protocols (e.g., IPv6 Source Guard) as described below:
  ▪ If an NS message is received on an trusted interface, it is forwarded without
      further processing.
  ▪ If an NS message is received on an untrusted interface, and the address
      prefix does not match any entry in the prefix table, it drops the packet.
  ▪ If the message does match an entry in the prefix table, it adds an entry to
      the dynamic user binding table after a fixed delay, and forwards the packet.
      Each entry in the dynamic binding table includes the link-layer address,
      IPv6 address, lifetime, as well as the VLAN and port interface which received
      the message.
  ▪ If an RA message is received in response to the original NS message
      (indicating a duplicate address) before the dynamic binding timeout period
      expires, the entry is deleted. Otherwise, when the timeout expires, the
      entry is dropped if the auto-detection process is not enabled.
  ▪ If the auto-detection process is enabled, the switch periodically sends an
      NS message to determine is the client still exists. If it does not receive an RA
      message in response after the configured timeout, the entry is dropped. If
      the switch receives an RA message before the timeout expires, it resets the
      lifetime for the dynamic binding, and the auto-detection process resumes.
Example
This example enables ND snooping globally and on VLAN 1.

```
Console(config)#ipv6 nd snooping
Console(config)#ipv6 nd snooping vlan 1
Console(config)#
```

**ipv6 nd snooping auto-detect**
This command enables automatic validation of dynamic user binding table entries by periodically sending NS messages and awaiting NA replies. Use the no form to disable this feature.

**Syntax**
```
[no] ipv6 nd snooping auto-detect
```

**Default Setting**
Disabled

**Command Mode**
Global Configuration

**Command Usage**
If auto-detection is enabled, the switch periodically sends an NS message to determine if a client listed in the dynamic binding table still exists. If it does not receive an RA message in response after the configured timeout, the entry is dropped. If the switch receives an RA message before the timeout expires, it resets the lifetime for the dynamic binding, and the auto-detection process resumes.

**Example**
```
Console(config)#ipv6 nd snooping auto-detect
Console(config)#
```

**ipv6 nd snooping auto-detect retransmit count**
This command sets the number of times the auto-detection process sends an NS message to determine if a dynamic user binding is still valid. Use the no form to restore the default setting.

**Syntax**
```
ipv6 nd snooping auto-detect retransmit count retransmit-times
no ipv6 nd snooping auto-detect retransmit count retransmit-times
```

**Default Setting**
3
**Command Mode**
Global Configuration

**Command Usage**
The timeout after which the switch will delete a dynamic user binding if no RA message is received is set to the retransmit count x the retransmit interval (see the `ipv6 nd snooping auto-detect retransmit interval` command). Based on the default settings, this is 3 seconds.

**Example**
```
Console(config)#ipv6 nd snooping auto-detect retransmit count 5
Console(config)#
```

**ipv6 nd snooping auto-detect retransmit interval**
This command sets the interval between which the auto-detection process sends NS messages to determine if a dynamic user binding is still valid. Use the `no` form to restore the default setting.

**Syntax**
```
ipv6 nd snooping auto-detect retransmit interval retransmit-interval
no ipv6 nd snooping auto-detect retransmit interval
```
- `retransmit-interval` – The interval between which the switch sends an NS message to determine if a client still exists. (Range: 1-10 seconds)

**Default Setting**
1 second

**Command Mode**
Global Configuration

**Command Usage**
The timeout after which the switch will delete a dynamic user binding if no RA message is received is set to the retransmit count (see the `ipv6 nd snooping auto-detect retransmit count` command) x the retransmit interval. Based on the default settings, this is 1 seconds.

**Example**
```
Console(config)#ipv6 nd snooping auto-detect retransmit interval 5
Console(config)#
```
**ipv6 nd snooping prefix timeout**

This command sets the time to wait for an RA message before deleting an entry in the prefix table. Use the **no** form to restore the default setting.

**Syntax**

```
ipv6 nd snooping prefix timeout timeout
no ipv6 nd snooping prefix timeout
```

`timeout` – The time to wait for an RA message to confirm that a prefix entry is still valid. (Range: 3-1800 seconds)

**Default Setting**

Set to the valid lifetime field in received RA packet

**Command Mode**

Global Configuration

**Command Usage**

If ND snooping is enabled and an RA message is received on a trusted interface, the switch will add an entry in the prefix table based upon the Prefix Information contained in the message. If an RA message is not received for a table entry with the same prefix for the specified timeout period, the entry is deleted.

**Example**

```
Console(config)#ipv6 nd snooping prefix timeout 200
Console(config)#
```

**ipv6 nd snooping max-binding**

This command sets the maximum number of address entries in the dynamic user binding table which can be bound to a port. Use the **no** form to restore the default setting.

**Syntax**

```
ipv6 nd snooping max-binding max-bindings
no ipv6 nd snooping max-binding
```

`max-bindings` – The maximum number of address entries in the dynamic user binding table which can be bound to a port. (Range: 1-5)

**Default Setting**

5

**Command Mode**

Interface Configuration (Ethernet, Port Channel)
**Example**

```
Console(config)#ipv6 nd snooping max-binding 200
Console(config)#
```

**ipv6 nd snooping trust**  This command configures a port as a trusted interface from which prefix information in RA messages can be added to the prefix table, or NS messages can be forwarded without validation. Use the `no` form to restore the default setting.

**Syntax**

```
[no] ipv6 nd snooping trust
```

**Default Setting**

Not trusted

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- In general, interfaces facing toward to the network core, or toward routers supporting the Network Discovery protocol, are configured as trusted interfaces.

- RA messages received from a trusted interface are added to the prefix table and forwarded toward their destination.

- NS messages received from a trusted interface are forwarded toward their destination. Nothing is added to the dynamic user binding table.

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 nd snooping trust
Console(config-if)#
```

**clear ipv6 nd snooping binding**  This command clears all entries in the dynamic user address binding table.

**Syntax**

```
clear ipv6 nd snooping binding
```

**Command Mode**

Privileged Exec
### Chapter 26 | IP Interface Commands

#### ND Snooping

**Example**

```plaintext
Console#clear ipv6 nd snooping binding
Console#show ipv6 nd snooping binding
MAC Address    IPv6 Address                           Lifetime   VLAN Interface
-------------- -------------------------------------- ---------- ---- ---------

Console#
```

**clear ipv6 nd snooping prefix**

This command clears all entries in the address prefix table.

**Syntax**

```
clear ipv6 nd snooping prefix [interface vlan vlan-id]
```

`vlan-id` - VLAN ID. (Range: 1-4094)

**Command Mode**

Privileged Exec

**Example**

```plaintext
Console#clear ipv6 nd snooping prefix
Console#show ipv6 nd snooping prefix
Prefix entry timeout: (seconds)
Prefix                                 Len Valid-Time Expire     VLAN Interface
-------------------------------------- --- ---------- ---------- ---- ---------

Console#
```

**show ipv6 nd snooping**

This command shows the configuration settings for ND snooping.

**Syntax**

```
show ipv6 nd snooping
```

**Command Mode**

Privileged Exec

**Example**

```plaintext
Console#show ipv6 nd snooping
Global ND Snooping status: enabled
ND Snooping auto-detection: disabled
ND Snooping auto-detection retransmit count: 3
ND Snooping auto-detection retransmit interval: 1 (second)
ND Snooping is configured on the following VLANs:
VLAN 1,
---
Interface     Trusted      Max-binding
---------     ----------     -----------
Eth 1/1       Yes           1
Eth 1/2       No            5
Eth 1/3       No            5
Eth 1/4       No            5
Eth 1/5       No            5
```
show ipv6 nd snooping binding

This command shows all entries in the dynamic user binding table.

Syntax

   show ipv6 nd snooping binding

Command Mode

Privileged Exec

Example

```
Console#show ipv6 nd snooping binding
MAC Address    IPv6 Address                           Lifetime   VLAN Interface
-------------- -------------------------------------- ---------- ---- ---------
0013-49aa-3926 2001:b001::211:95ff:fe84:cb9e                 100    1 Eth 1/1
0012-cf01-0203 2001::1                                      3400    2 Eth 1/2
Console#
```

show ipv6 nd snooping prefix

This command shows all entries in the address prefix table.

Syntax

   show ipv6 nd snooping prefix [interface vlan vlan-id]

   vlan-id - VLAN ID. (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 nd snooping prefix
Prefix entry timeout: 100 (second)
Prefix                                           Len Valid-Time Expire  VLAN Interface
------------------------------------------------- ---------- ---------- ---- ---------
2001:b000::                                  64 2592000        100    1 Eth 1/1
2001::                                      64   600          34    2 Eth 1/2
Console#
```
After network interfaces are configured for the switch, the paths used to send traffic between different interfaces must be set. If routing is enabled on the switch, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for static routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

**Table 203: IP Routing Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Routing Configuration</td>
<td>Configures global parameters for static routing, displays the routing table and statistics for protocols used to exchange routing information</td>
</tr>
</tbody>
</table>

**Global Routing Configuration**

**Table 204: Global Routing Configuration Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route</td>
<td>Configures static routes</td>
<td>GC</td>
</tr>
<tr>
<td>ip sw-route</td>
<td>Uses software to process static routes</td>
<td>GC</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays specified entries in the routing table</td>
<td>PE</td>
</tr>
<tr>
<td>show ip route database</td>
<td>Displays static entries in the routing table</td>
<td>PE</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Displays summary information for the routing table</td>
<td>PE</td>
</tr>
</tbody>
</table>
IPv4 Commands

**ip route**  This command configures static routes. Use the **no** form to remove static routes.

**Syntax**

```
ip route destination-ip netmask next-hop [distance]
no ip route {destination-ip netmask [next-hop] | *}
```

- **destination-ip** – IP address of the destination network, subnetwork, or host.
- **netmask** - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **next-hop** – IP address of the next hop router used for this route.
- **distance** – An administrative distance for the route. (Range: 1-255, Default: 1)
- ***** – Removes all static routing table entries.

**Default Setting**
No static routes are configured.

**Command Mode**
Global Configuration

**Command Usage**
Up to 24 static routes can be configured.

**Example**
This example forwards all traffic for subnet 192.168.1.0 to the gateway router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

**ip sw-route**  This command using software to process static routes. Use the **no** form to disable this function.

**Syntax**

```
[no] ip sw-route
```

**Default Setting**
Hardware is used to process static routes.

**Command Mode**
Global Configuration
Command Usage
◆ Due to a hardware limitation on the EX-3548, static routes do not work with DiffServ. Hardware processing of static routes is enabled by default. If you must use DiffServ, then use this command to configure the switch to process static routes through software.
◆ The switch can only process 200~300 routing packets/second. So, it should only be used as L3 switch in this mode for light routing requirements.

Example

```
Console(config)#ip sw-route
Console(config)#
```

**show ip route**  This command displays information in the Forwarding Information Base (FIB).

**Syntax**

```
show ip route [connected | database | static | summary]
```

- **connected** – Displays all currently connected entries.
- **database** – All known routes, including inactive routes.
- **static** – Displays all static entries.
- **summary** – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

**Command Mode**
Privileged Exec

**Command Usage**
◆ The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

◆ This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN
interface associated with any static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the show ip route database command.

Example

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default

C       192.168.1.0/24 is directly connected, VLAN1
```

```
show ip route database
This command displays entries in the Routing Information Base (RIB).

Command Mode
Privileged Exec

Command Usage
The RIB contains all available routes learned through directly attached networks, and any additionally configured routes such as static routes. The RIB contains the set of all available routes from which optimal entries are selected for use by the Forwarding Information Base (see Command Usage under the show ip route command).

Example

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      > - selected route, * - FIB route, p - stale info

C    *> 192.168.1.0/24 is directly connected, VLAN1
```

```
```

Console#
show ip route summary

This command displays summary information for the routing table.

**Command Mode**
Privileged Exec

**Example**
In the following example, the numeric identifier following the named routing table (that is, the Forwarding Information Base) is the FIB ID.

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 1
Connected       2
Total           2
Console#
```
Appendices

This section provides additional information and includes these items:

◆ “Troubleshooting” on page 779

◆ “License Information” on page 781

◆ “Customer Support” on page 793
Troubleshooting

Problems Accessing the Management Interface

Table 205: Troubleshooting Chart

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot connect using Telnet, web browser, or SNMP software</td>
<td>- Be sure the switch is powered up.</td>
</tr>
<tr>
<td></td>
<td>- Check network cabling between the management station and the switch.</td>
</tr>
<tr>
<td></td>
<td>- Check that you have a valid network connection to the switch and the port you are using has not been disabled.</td>
</tr>
<tr>
<td></td>
<td>- Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask, and default gateway.</td>
</tr>
<tr>
<td></td>
<td>- Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.</td>
</tr>
<tr>
<td></td>
<td>- If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.</td>
</tr>
<tr>
<td></td>
<td>- If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.</td>
</tr>
<tr>
<td>Cannot connect using Secure Shell</td>
<td>- If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.</td>
</tr>
<tr>
<td></td>
<td>- Be sure the control parameters for the SSH server are properly configured on the switch.</td>
</tr>
<tr>
<td></td>
<td>- Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service.</td>
</tr>
<tr>
<td></td>
<td>- Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.</td>
</tr>
<tr>
<td></td>
<td>- Be sure you have imported the client’s public key to the switch (if public key authentication is used).</td>
</tr>
<tr>
<td>Cannot access the onboard configuration program via a serial port connection</td>
<td>- Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps).</td>
</tr>
<tr>
<td></td>
<td>- Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.</td>
</tr>
<tr>
<td>Forgot or lost the password</td>
<td>- Contact your local distributor.</td>
</tr>
</tbody>
</table>
Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the “show tech-support” command to record all system settings in this file.
9. Contact your distributor’s service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
```
This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 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 Library 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

1. 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.

2. 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.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, 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). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, 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 Program, 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 Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) 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; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, 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 executable. 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.

If distribution of executable or 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 counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program 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.

6. 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 Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program 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.

8. 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 Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program 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 Program.

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.
9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program 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.

10. The Free Software Foundation may publish revised and/or new versions of the 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 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 Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, 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

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, 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.

2. 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 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.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License, version 3.0

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.
Appendix B
License Information

GNU Lesser General Public License, version 3.0

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:
Appendix B | License Information

The BSD License

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user’s computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.
The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

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.

Open Source Software Used

The Zebra Support Web site, located at http://www.zebra.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>URL</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>u-boot</td>
<td>1.3</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>linux</td>
<td>2.6.22.18</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>busybox</td>
<td>1.7.0</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>glibc</td>
<td>2.5</td>
<td><a href="http://www.gnu.org/software/libc/">http://www.gnu.org/software/libc/</a></td>
<td>GNU GPL</td>
</tr>
<tr>
<td>dhcp</td>
<td></td>
<td><a href="http://www.isc.org/software/dhcp">http://www.isc.org/software/dhcp</a></td>
<td>Internet Systems Consortium</td>
</tr>
<tr>
<td>netsnmp</td>
<td>5.1</td>
<td><a href="http://www.net-snmp.org/">http://www.net-snmp.org/</a></td>
<td>BSD-style</td>
</tr>
<tr>
<td>openssh</td>
<td></td>
<td><a href="http://www.openssh.com/">http://www.openssh.com/</a></td>
<td>BSD-style</td>
</tr>
<tr>
<td>openssl</td>
<td></td>
<td><a href="http://www.openssl.org/">http://www.openssl.org/</a></td>
<td>BSD-style</td>
</tr>
<tr>
<td>tftp-hpa</td>
<td></td>
<td><a href="http://sourceforge.net/projects/libtacplus">http://sourceforge.net/projects/libtacplus</a></td>
<td>BSD-style</td>
</tr>
<tr>
<td>radiusclient</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>libtacplus</td>
<td></td>
<td></td>
<td>GNU GPL</td>
</tr>
<tr>
<td>cdp</td>
<td>0.5.7</td>
<td><a href="http://packages.debian.org/search?keywords=lldpd">http://packages.debian.org/search?keywords=lldpd</a></td>
<td>Internet Systems Consortium (cdp is part of lldpd 0.5.7)</td>
</tr>
<tr>
<td>Zebos5</td>
<td>7.4.0-t40</td>
<td>IP Infusion</td>
<td>IPI-proprietary</td>
</tr>
</tbody>
</table>

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
License Information

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.

SNMP License (netsnmp5.1)
Various copyrights apply to this package, listed in various separate parts below. Please make sure
that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----
Copyright 1996, 1998-2000 The Regents of the University of California
All Rights Reserved
Permission to use, copy, modify and distribute this software and its documentation for any purpose
and without fee is hereby granted, provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in supporting documentation, and
that the name of CMU and The Regents of the University of California not be used in advertising or
publicity pertaining to distribution of the software without specific written permission.
CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE
UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL
DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE 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.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----
Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the
  following disclaimer.

* 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.

* Neither the name of the Networks Associates Technology, Inc 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 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 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 DAMAGE.
--- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 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.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``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 COPYRIGHT HOLDER 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.

--- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 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.

* Neither the name of the Sun Microsystems, Inc. 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 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 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 DAMAGE.
---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2009, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* 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.
* Neither the name of Sparta, Inc 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 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 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 DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* 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.
* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY 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 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 DAMAGE.
--- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 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.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "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 COPYRIGHT HOLDER 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.

--- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. 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. Neither the name of Apple Inc. ("Apple") 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 APPLE AND ITS 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 APPLE 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.
Appendix B | License Information

ISC License

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* 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.
* Neither the name of ScienceLogic, LLC 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 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 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 DAMAGE.

-------------------------------------------------------------------------------------------------------------------------------------

Last modified: Thursday, 26-May-2011 23:21:31 UTC
For questions regarding web content and site functionality, please write to the net-snmp-users mail list.
Customer Support

Zebra Support

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 is available at: http://www.zebra.com/support.

When contacting support, please provide the following information:
◆ Serial number of the unit
◆ Model number or product name
◆ Software type and version number

Support responds to calls by e-mail, telephone or fax 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

Support, located at http://www.zebra.com/support provides information and online assistance including developer tools, software downloads, product manuals, and online repair requests.

Manuals

Documentation is available at: http://www.zebra.com/support.
Glossary

ACL  Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP  Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP  Boot Protocol is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS  Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP  Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP Snooping  A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DiffServ  Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.
<table>
<thead>
<tr>
<th>Glossary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DNS</strong></td>
<td>Domain Name Service. A system used for translating host names for network nodes into IP addresses.</td>
</tr>
<tr>
<td><strong>DSCP</strong></td>
<td>Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.</td>
</tr>
<tr>
<td><strong>EAPOL</strong></td>
<td>Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.</td>
</tr>
<tr>
<td><strong>EUI</strong></td>
<td>Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.</td>
</tr>
<tr>
<td><strong>GARP</strong></td>
<td>Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.</td>
</tr>
<tr>
<td><strong>GMRP</strong></td>
<td>Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.</td>
</tr>
<tr>
<td><strong>GVRP</strong></td>
<td>GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.</td>
</tr>
<tr>
<td><strong>ICMP</strong></td>
<td>Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.</td>
</tr>
</tbody>
</table>
IEEE 802.1D  Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q  VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p  An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s  An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1w  An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X  Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac  Defines frame extensions for VLAN tagging.

IEEE 802.3x  Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP  Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

IGMP Query  On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP Proxy  Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in an simple tree that uses IGMP Proxy.
**Glossary**

**IGMP Snooping**  
Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

**In-Band Management**  
Management of the network from a station attached directly to the network.

**IP Multicast Filtering**  
A process whereby this switch can pass multicast traffic along to participating hosts.

**IP Precedence**  
The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

**LACP**  
Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

**Layer 2**  
Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

**Link Aggregation**  
*See Port Trunk.*

**LLDP**  
Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

**MD5**  
Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

**MIB**  
Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

**MSTP**  
Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.
**MRD**  Multicast Router Discovery is a protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

**Multicast Switching**  A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

**MVR**  Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as television channels or video-on-demand, across a service-provider’s network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

**NTP**  Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

**OAM**  Operation, Administration, and Maintenance provides remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

**Out-of-Band Management**  Management of the network from a station not attached to the network.

**Port Authentication**  See IEEE 802.1X.

**Port Mirroring**  A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

**Port Trunk**  Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

**QinQ**  QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.
**QoS**  Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

**RADIUS**  Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

**RMON**  Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

**RSTP**  Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

**SMTP**  Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

**SNMP**  Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

**SNTP**  Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

**SSH**  Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

**STA**  Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated orbackup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

**TACACS+**  Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.
TCP/IP  Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Telnet  Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP  Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP  User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC  Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN  Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem  A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.
Index of CLI Commands

A
B
C
D
E
F
G
H
I
J
L
M
N
P
Q
R
S
T
U
V
W

A
aaa accounting commands
aaa accounting dot1x
aaa accounting exec
aaa accounting update
aaa authorization commands
aaa authorization exec
aaa group server
absolute
access-list arp
access-list ip
access-list ipv6
access-list mac
accounting commands
accounting dot1x
accounting exec
adoptd upgrade
alias
arp
authentication enable
authentication login
authorization commands
authorization exec
auto-traffic-control
auto-traffic-control action
auto-traffic-control alarm-clear-threshold
auto-traffic-control alarm-fire-threshold
auto-traffic-control apply-timer
auto-traffic-control auto-control-release
auto-traffic-control control-release
auto-traffic-control release-timer
boot system
bridge-ext gvrp
calendar set
capabilities
cdp (Global Configuration)
cdp (Interface Configuration)
cdp hold-time
cdp transmit-interval
cdp version
Index of CLI Commands

channel-group 406
class 558
class-map 554
clear access-list hardware counters 373
clear arp-cache 733
clear cdp table 702
clear counters 385
clear dns cache 710
clear host 710
clear ip dhcp snooping binding 307
clear ip dhcp snooping database flash 307
clear ip igmp snooping groups dynamic 588
clear ip igmp snooping statistics 589
clear ip source-guard binding blocked 323
clear ipv6 dhcp snooping binding 316
clear ipv6 dhcp snooping statistics 317
clear ipv6 mld snooping groups dynamic 617
clear ipv6 mld snooping statistics 617
clear ipv6 nd snooping binding 767
clear ipv6 nd snooping prefix 768
clear ipv6 neighbors 759
clear ipv6 traffic 753
clear log 135
clear mac-address-table dynamic 461
clear mvr groups dynamic 643
clear mvr statistics 643
clear mvr6 groups dynamic 665
clear mvr6 statistics 666
clear network-access 288
clear pppoe intermediate-agent statistics 267
clock summer-time (date) 149
clock summer-time (predefined) 150
clock summer-time (recurring) 151
clock timezone 153
cluster 159
cluster commander 160
cluster ip-pool 161
cluster member 161
configure 93
controller hello-interval adjacency-hold-time 166
controller host ip address 166
copy 110
databits 121
debug adoption 168
delete 113
delete public-key 240
description 555
description 381
dir 114
disable 94
disconnect 129
dos-protection echo-chargen 341
dos-protection smurf 341
dos-protection tcp-flooding 342
dos-protection tcp-null-scan 342
dos-protection tcp-syn-fin-scan 343
dos-protection tcp-udp-port-zero 343
dos-protection tcp-xmas-scan 344
dos-protection udp-flooding 344
dos-protection win-nuke 345
dot1q-tunnel system-tunnel-control 515
dot1q-tunnel tpid 516
dot1x default 245
dot1x eapol-pass-through 246
dot1x identity profile 254
dot1x intrusion-action 247
dot1x max-reauth-req 248
dot1x max-req 248
dot1x max-start 254
dot1x operation-mode 249
dot1x pae supplicant 255
dot1x port-control 250
dot1x re-authenticate 253
dot1x re-authentication 250
dot1x system-auth-control 247
dot1x timeout auth-period 256
dot1x timeout held-period 256
dot1x timeout quiet-period 251
dot1x timeout re-authperiod 251
dot1x timeout start-period 257
dot1x timeout supp-timeout 252
dot1x timeout tx-period 252
enable 91
enable password 204
end 95
exec-timeout 122
exit 95
flowcontrol 381
garp timer 497
hostname 98
interface 378
interface vlan 504
ip access-group 356
ip address 724
ip arp inspection 332
ip arp inspection filter 333
ip arp inspection limit 337
ip arp inspection log-buffer logs 334
ip arp inspection trust 337
ip arp inspection validate 335
ip arp inspection vlan 336
ip default-gateway 726
ip dhcp client class-id 714
ip dhcp relay server 720
ip dhcp restart client 715
ip dhcp restart relay 721
ip dhcp snooping 297
ip dhcp snooping database flash 308
ip dhcp snooping information option 299
ip dhcp snooping information option circuit-id 305
ip dhcp snooping information option encode no-subtype 300
ip dhcp snooping information option remote-id 301
ip dhcp snooping information policy 302
ip dhcp snooping limit rate 303
ip dhcp snooping trust 306
ip dhcp snooping verify mac-address 303
ip dhcp snooping vlan 304
ip domain-list      705
ip domain-lookup    706
ip domain-name      707
ip host             708
ip http port        229
ip http secure-port 230
ip http secure-server 231
ip http server      230
ip igmp authentication 599
ip igmp filter (Global Configuration) 597
ip igmp filter (Interface Configuration) 601
ip igmp max-groups 601
ip igmp max-groups action 602
ip igmp profile     597
ip igmp query-drop 603
ip igmp snooping     573
ip igmp snooping priority 574
ip igmp snooping proxy-reporting 574
ip igmp snooping querier 575
ip igmp snooping router-alert-option-check 576
ip igmp snooping router-port-expire-time 576
ip igmp snooping tcn-flood 577
ip igmp snooping tcn-query-solicit 578
ip igmp snooping unregistered-data-flood 579
ip igmp snooping unsolicited-report-interval 579
ip igmp snooping version 580
ip igmp snooping version-exclusive 581
ip igmp snooping vlan general-query-suppression 581
ip igmp snooping vlan immediate-leave 582
ip igmp snooping vlan last-memb-query-count 583
ip igmp snooping vlan last-memb-query-intvl 583
ip igmp snooping vlan mrd 584
ip igmp snooping vlan mrouter 595
ip igmp snooping vlan proxy-address 585
ip igmp snooping vlan query-interval 586
ip igmp snooping vlan query-resp-intvl 587
ip igmp snooping vlan static 588
ip multicast-data-drop 603
ip name-server      708
ip proxy-arp         732
ip route             772
ip source-guard      321
ip source-guard binding 319
ip source-guard max-binding 323
ip source-guard mode 324
ip ssh authentication-retries 237
ip ssh crypto host-key generator 240
ip ssh crypto zeroize 241
ip ssh save host-key 242
ip ssh server        238
ip ssh server-key size 239
ip ssh timeout       239
ip sw-route          772
ip telnet max-sessions 233
ip telnet port       233
ip telnet server     234
ip tftp retry        118
ip tftp timeout      119
ipv6 access-group    362
ipv6 address         736
ipv6 address autoconfig 737
ipv6 address eui-64 739
ipv6 address link-local 741
ipv6 default-gateway 735
ipv6 dhcp client rapid-commit vlan 716
ipv6 dhcp restart client vlan 717
ipv6 dhcp snooping 310
ipv6 dhcp snooping max-binding 315
ipv6 dhcp snooping option remote-id 312
ipv6 dhcp snooping option remote-id policy 313
ipv6 dhcp snooping trust 315
ipv6 dhcp snooping vlan 314
ipv6 enable          742
ipv6 host            709
ipv6 mld filter (Global Configuration) 622
ipv6 mld filter (Interface Configuration) 624
ipv6 mld max-groups 625
ipv6 mld max-groups action 626
ipv6 mld profile 622
ipv6 mld query-drop 626
ipv6 mld snooping 609
ipv6 mld snooping proxy-reporting 611
ipv6 mld snooping querier 609
ipv6 mld snooping query-interval 610
ipv6 mld snooping query-max-response-time 611
ipv6 mld snooping robustness 612
ipv6 mld snooping router-port-expire-time 612
ipv6 mld snooping unknown-multicast mode 613
ipv6 mld snooping unsolicited-report-interval 613
ipv6 mld snooping version 614
ipv6 mld snooping vlan immediate-leave 615
ipv6 mld snooping vlan mrouter 615
ipv6 mld snooping vlan static 616
ipv6 mtu 743
ipv6 multicast-data-drop 627
ipv6 nd dad attempts 755
ipv6 nd ns-interval 756
ipv6 nd raguard 757
ipv6 nd reachable-time 758
ipv6 nd snooping 762
ipv6 nd snooping auto-detect 764
ipv6 nd snooping auto-detect retransmit count 764
ipv6 nd snooping auto-detect retransmit interval 765
ipv6 nd snooping max-binding 766
ipv6 nd snooping prefix timeout 766
ipv6 nd snooping trust 767
ipv6 source-guard 328
ipv6 source-guard binding 326
ipv6 source-guard max-binding 329
jumbo frame         107
l2protocol-tunnel tunnel-dmac 521
lacp 406
lacp admin-key (Ethernet Interface) 408
lacp admin-key (Port Channel) 410
lacp port-priority 409
lacp system-priority 410
lacp timeout        411
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>121</td>
</tr>
<tr>
<td>lldp admin-status</td>
<td>679</td>
</tr>
<tr>
<td>lldp basic-tlv management-ip-address</td>
<td>679</td>
</tr>
<tr>
<td>lldp basic-tlv port-description</td>
<td>680</td>
</tr>
<tr>
<td>lldp basic-tlv system-capabilities</td>
<td>680</td>
</tr>
<tr>
<td>lldp basic-tlv system-description</td>
<td>681</td>
</tr>
<tr>
<td>lldp basic-tlv system-name</td>
<td>681</td>
</tr>
<tr>
<td>lldp dot1-tlv proto-ident</td>
<td>682</td>
</tr>
<tr>
<td>lldp dot1-tlv proto-vid</td>
<td>682</td>
</tr>
<tr>
<td>lldp dot1-tlv pvid</td>
<td>683</td>
</tr>
<tr>
<td>lldp dot1-tlv vlan-name</td>
<td>683</td>
</tr>
<tr>
<td>lldp dot3-tlv link-agg</td>
<td>684</td>
</tr>
<tr>
<td>lldp dot3-tlv mac-phy</td>
<td>684</td>
</tr>
<tr>
<td>lldp dot3-tlv max-frame</td>
<td>685</td>
</tr>
<tr>
<td>lldp dot3-tlv poe</td>
<td>685</td>
</tr>
<tr>
<td>lldp holdtime-multiplier</td>
<td>675</td>
</tr>
<tr>
<td>lldp med-fast-start-count</td>
<td>676</td>
</tr>
<tr>
<td>lldp med-location civic-addr</td>
<td>686</td>
</tr>
<tr>
<td>lldp med-notification</td>
<td>688</td>
</tr>
<tr>
<td>lldp med-tlv ext-poe</td>
<td>688</td>
</tr>
<tr>
<td>lldp med-tlv inventory</td>
<td>689</td>
</tr>
<tr>
<td>lldp med-tlv location</td>
<td>689</td>
</tr>
<tr>
<td>lldp med-tlv med-cap</td>
<td>690</td>
</tr>
<tr>
<td>lldp med-tlv network-policy</td>
<td>690</td>
</tr>
<tr>
<td>lldp notification</td>
<td>691</td>
</tr>
<tr>
<td>lldp notification-interval</td>
<td>676</td>
</tr>
<tr>
<td>lldp refresh-interval</td>
<td>677</td>
</tr>
<tr>
<td>lldp reinit-delay</td>
<td>677</td>
</tr>
<tr>
<td>lldp tx-delay</td>
<td>678</td>
</tr>
<tr>
<td>logging facility</td>
<td>131</td>
</tr>
<tr>
<td>logging history</td>
<td>132</td>
</tr>
<tr>
<td>logging host</td>
<td>133</td>
</tr>
<tr>
<td>logging on</td>
<td>133</td>
</tr>
<tr>
<td>logging sendmail</td>
<td>138</td>
</tr>
<tr>
<td>logging sendmail destination-email</td>
<td>140</td>
</tr>
<tr>
<td>logging sendmail host</td>
<td>138</td>
</tr>
<tr>
<td>logging sendmail level</td>
<td>139</td>
</tr>
<tr>
<td>logging sendmail source-email</td>
<td>140</td>
</tr>
<tr>
<td>logging trap</td>
<td>134</td>
</tr>
<tr>
<td>login</td>
<td>123</td>
</tr>
<tr>
<td>loopback detection trap</td>
<td>456</td>
</tr>
<tr>
<td>loopback-detection</td>
<td>454</td>
</tr>
<tr>
<td>loopback-detection action</td>
<td>454</td>
</tr>
<tr>
<td>loopback-detection recover-time</td>
<td>455</td>
</tr>
<tr>
<td>loopback-detection release</td>
<td>457</td>
</tr>
<tr>
<td>loopback-detection transmit-interval</td>
<td>456</td>
</tr>
<tr>
<td>mac access-group</td>
<td>369</td>
</tr>
<tr>
<td>mac-address-table aging-time</td>
<td>459</td>
</tr>
<tr>
<td>mac-address-table static</td>
<td>460</td>
</tr>
<tr>
<td>mac-authentication intrusion-action</td>
<td>287</td>
</tr>
<tr>
<td>mac-authentication max-mac-count</td>
<td>287</td>
</tr>
<tr>
<td>mac-authentication reauth-time</td>
<td>279</td>
</tr>
<tr>
<td>mac-learning</td>
<td>272</td>
</tr>
<tr>
<td>mac-vlan</td>
<td>532</td>
</tr>
<tr>
<td>management</td>
<td>260</td>
</tr>
<tr>
<td>match</td>
<td>556</td>
</tr>
<tr>
<td>max-hops</td>
<td>474</td>
</tr>
<tr>
<td>media-type</td>
<td>382</td>
</tr>
<tr>
<td>memory</td>
<td>192</td>
</tr>
<tr>
<td>mst priority</td>
<td>474</td>
</tr>
<tr>
<td>mst vlan</td>
<td>475</td>
</tr>
<tr>
<td>mvr</td>
<td>631</td>
</tr>
<tr>
<td>mvr associated-profile</td>
<td>631</td>
</tr>
<tr>
<td>mvr domain</td>
<td>632</td>
</tr>
<tr>
<td>mvr group</td>
<td>633</td>
</tr>
<tr>
<td>mvr immediate-leave</td>
<td>640</td>
</tr>
<tr>
<td>mvr priority</td>
<td>633</td>
</tr>
<tr>
<td>mvr profile</td>
<td>634</td>
</tr>
<tr>
<td>mvr proxy-query-interval</td>
<td>635</td>
</tr>
<tr>
<td>mvr proxy-switching</td>
<td>636</td>
</tr>
<tr>
<td>mvr robustness-value</td>
<td>637</td>
</tr>
<tr>
<td>mvr source-port-mode dynamic</td>
<td>637</td>
</tr>
<tr>
<td>mvr type</td>
<td>641</td>
</tr>
<tr>
<td>mvr upstream-source-ip</td>
<td>638</td>
</tr>
<tr>
<td>mvr vlan</td>
<td>639</td>
</tr>
<tr>
<td>mvr vlan group</td>
<td>642</td>
</tr>
<tr>
<td>mvr6 associated-profile</td>
<td>655</td>
</tr>
<tr>
<td>mvr6 domain</td>
<td>655</td>
</tr>
<tr>
<td>mvr6 immediate-leave</td>
<td>662</td>
</tr>
<tr>
<td>mvr6 priority</td>
<td>656</td>
</tr>
<tr>
<td>mvr6 profile</td>
<td>657</td>
</tr>
<tr>
<td>mvr6 proxy-query-interval</td>
<td>658</td>
</tr>
<tr>
<td>mvr6 proxy-switching</td>
<td>658</td>
</tr>
<tr>
<td>mvr6 robustness-value</td>
<td>659</td>
</tr>
<tr>
<td>mvr6 source-port-mode dynamic</td>
<td>660</td>
</tr>
<tr>
<td>mvr6 type</td>
<td>663</td>
</tr>
<tr>
<td>mvr6 upstream-source-ip</td>
<td>661</td>
</tr>
<tr>
<td>mvr6 vlan</td>
<td>661</td>
</tr>
<tr>
<td>mvr6 vlan group</td>
<td>664</td>
</tr>
<tr>
<td>name</td>
<td>476</td>
</tr>
<tr>
<td>negotiation</td>
<td>383</td>
</tr>
<tr>
<td>network-access aging</td>
<td>278</td>
</tr>
<tr>
<td>network-access dynamic-qos</td>
<td>280</td>
</tr>
<tr>
<td>network-access dynamic-vlan</td>
<td>281</td>
</tr>
<tr>
<td>network-access guest-vlan</td>
<td>282</td>
</tr>
<tr>
<td>network-access link-detection</td>
<td>282</td>
</tr>
<tr>
<td>network-access link-detection link-down</td>
<td>283</td>
</tr>
<tr>
<td>network-access link-detection link-up</td>
<td>283</td>
</tr>
<tr>
<td>network-access link-detection link-up-down</td>
<td>284</td>
</tr>
<tr>
<td>network-access mac-filter</td>
<td>278</td>
</tr>
<tr>
<td>network-access max-mac-count</td>
<td>284</td>
</tr>
<tr>
<td>network-access mode mac-authentication</td>
<td>285</td>
</tr>
<tr>
<td>network-access port-mac-filter</td>
<td>286</td>
</tr>
<tr>
<td>nlm</td>
<td>189</td>
</tr>
<tr>
<td>no adoption</td>
<td>168</td>
</tr>
<tr>
<td>no rspan session</td>
<td>433</td>
</tr>
<tr>
<td>ntp authenticate</td>
<td>145</td>
</tr>
<tr>
<td>ntp authentication-key</td>
<td>146</td>
</tr>
<tr>
<td>ntp client</td>
<td>147</td>
</tr>
<tr>
<td>ntp server</td>
<td>147</td>
</tr>
<tr>
<td>parity</td>
<td>124</td>
</tr>
<tr>
<td>password</td>
<td>124</td>
</tr>
<tr>
<td>password-thresh</td>
<td>125</td>
</tr>
<tr>
<td>periodic</td>
<td>157</td>
</tr>
<tr>
<td>permit, deny</td>
<td>598</td>
</tr>
<tr>
<td>permit, deny</td>
<td>623</td>
</tr>
<tr>
<td>permit, deny (ARP ACL)</td>
<td>371</td>
</tr>
</tbody>
</table>
Index of CLI Commands

permit, deny (Extended IPv4 ACL) 354
permit, deny (Extended IPv6 ACL) 360
permit, deny (Standard IP ACL) 353
permit, deny (Standard IPv6 ACL) 359
permit, deny (MAC ACL) 365
ping 730
ping6 753
police flow 559
police srtcm-color 561
police trtcm-color 563
policy-map 557
port monitor 425
port security 273
port-channel load-balance 404
power inline 419
power inline compatible 417
power inline maximum allocation 420
power inline priority 421
power inline time-range 422
power mainpower maximum allocation 418
power-save 401
pppoe intermediate-agent 263
pppoe intermediate-agent format-type 263
pppoe intermediate-agent port-enable 264
pppoe intermediate-agent port-format-type 265
pppoe intermediate-agent port-format-type remote-id-delimiter 266
pppoe intermediate-agent trust 266
pppoe intermediate-agent vendor-tag strip 267
privilege 207
process cpu 192
prompt 89
protocol-vlan protocol-group (Configuring Groups) 526
protocol-vlan protocol-group (Configuring Interfaces) 527
qos map cos-dscp 546
qos map dscp-mutation 548
qos map phb-queue 549
qos map trust-mode 550
queue mode 542
queue weight 543
quit 92
radius-server acct-port 210
radius-server auth-port 211
radius-server host 211
radius-server key 212
radius-server retransmit 213
radius-server timeout 213
range 598
range 623
rate-limit 436
rcommand 162
reload (Global Configuration) 90
reload (Privileged Exec) 94
rename 557
revision 476
rmon alarm 196
rmon collection history 198
rmon collection rmon1 199
rmon event 197
rspan destination 431
rspan remote vlan 432
rspan source 430
server 224
service-policy 568
set cos 565
set ip dscp 566
set phb 567
show access-group 374
show access-list 374
show access-list arp 372
show access-list tcam-utilization 99
show accounting 228
show adoption debug 168
show adoption history 169
show adoption status 170
show arp 733
show arp access-list 373
show auto-traffic-control 451
show auto-traffic-control interface 452
show bridge-ext 499
show cable-diagnostics 400
show calendar 154
show cdp 702
show cdp interface 703
show cdp neighbors 703
show class-map 569
show cluster 163
show cluster candidates 163
show cluster members 163
show dns 711
show dns cache 711
show dos-protection 345
show dot1q-tunnel 520
show dot1x 257
show garp timer 500
show gvrp configuration 501
show history 92
show hosts 712
show interfaces brief 386
show interfaces counters 386
show interfaces protocol-vlan protocol-group 528
show interfaces status 388
show interfaces switchport 389
show interfaces transceiver 397
show interfaces transceiver-threshold 398
show ip access-group 357
show ip access-list 357
show ip arp inspection configuration 338
show ip arp inspection interface 338
show ip arp inspection log 339
show ip arp inspection statistics 339
show ip arp inspection vlan 340
show ip dhcp snooping 308
show ip dhcp snooping binding 309
show ip igmp authentication 604
show ip igmp filter 604
Index of CLI Commands

show ip igmp profile 605
show ip igmp query-drop 606
show ip igmp snooping 589
show ip igmp snooping group 590
show ip igmp snooping mrouter 591
show ip igmp snooping statistics 592
show ip igmp throttle interface 606
show ip interface 727
show ip multicast-data-drop 607
show ip route 773
show ip route database 774
show ip route summary 775
show ip source-guard 325
show ip source-guard binding 325
show ip ssh 242
show ip telnet 234
show ip tftp 119
show ip traffic 727
show ipv6 access-group 363
show ipv6 access-list 363
show ipv6 default-gateway 744
show ipv6 dhcp duid 718
show ipv6 dhcp snooping 317
show ipv6 dhcp snooping binding 318
show ipv6 dhcp snooping statistics 318
show ipv6 dhcp vlan 719
show ipv6 interface 745
show ipv6 mld filter 627
show ipv6 mld profile 628
show ipv6 mld query-drop 628
show ipv6 mld snooping group 618
show ipv6 mld snooping group source-list 619
show ipv6 mld snooping mrouter 620
show ipv6 mld snooping statistics 620
show ipv6 mld throttle interface 629
show ipv6 mld snooping 618
show ipv6 mtu 747
show ipv6 nd raguard 759
show ipv6 nd snooping 768
show ipv6 nd snooping binding 769
show ipv6 nd snooping prefix 769
show ipv6 neighbors 760
show ipv6 source-guard 330
show ipv6 source-guard binding 331
show ipv6 traffic 747
show l2protocol-tunnel 525
show lacp 412
show line 130
show lldp config 692
show lldp info local-device 693
show lldp info remote-device 694
show lldp info statistics 695
show lldp neighbors 696
show log 135
show logging 136
show logging sendmail 141
show loopback-detection 458
show mac access-group 369
show mac access-list 370
show mac-address-table 461
show mac-address-table aging-time 462
show mac-address-table count 462
show mac-vlan 533
show management 261
show memory 100
show mvr associated-profile 645
show mvr interface 645
show mvr members 646
show mvr profile 648
show mvr statistics 648
show mvr6 666
show mvr6 associated-profile 667
show mvr6 interface 668
show mvr6 members 669
show mvr6 profile 670
show mvr6 statistics 671
show network-access 288
show network-access mac-address-table 289
show network-access mac-filter 290
show nlm oper-status 191
show ntp 148
show policy-map 569
show policy-map interface 570
show port monitor 428
show port security 275
show port-channel load-balance 415
show power inline status 423
show power inline time-range 424
show power mainpower 424
show power-save 402
show pppoe intermediate-agent info 268
show pppoe intermediate-agent statistics 269
show privilege 207
show process cpu 100
show protocol-vlan protocol-group 528
show public-key 243
show qos map cos-dscp 551
show qos map dscp-mutation 551
show qos map phb-queue 552
show qos map trust-mode 552
show queue mode 545
show queue weight 545
show radius-server 214
show reload 95
show rmon alarms 200
show rmon events 200
show rmon history 200
show rmon statistics 201
show rspan 434
show running-config 101
show snmp 175
show snmp engine-id 186
show snmp group 186
show snmp notify-filter 191
show snmp user 187
show snmp view 188
show snmp-server enable port-traps 180
show snmp 144
Index of CLI Commands

- show spanning-tree 490
- show spanning-tree mst configuration 493
- show ssh 244
- show startup-config 102
- show subnet-vlan 531
- show system 103
- show tacacs-server 217
- show tech-support 104
- show time-range 158
- show traffic-segmentation 350
- show upgrade 118
- show users 105
- show version 106
- show vlan 513
- show voice vlan 539
- show watchdog 107
- show web-auth 295
- show web-auth interface 295
- show web-auth summary 296
- shutdown 383
- silent-time 126
- snmp-server 173
- snmp-server community 173
- snmp-server contact 174
- snmp-server enable port-traps atc broadcast-alarm-clear 447
- snmp-server enable port-traps atc broadcast-alarm-fire 448
- snmp-server enable port-traps atc broadcast-control-apply 448
- snmp-server enable port-traps atc broadcast-control-release 449
- snmp-server enable port-traps atc multicast-alarm-clear 449
- snmp-server enable port-traps atc multicast-alarm-fire 450
- snmp-server enable port-traps atc multicast-control-apply 450
- snmp-server enable port-traps atc multicast-control-release 451
- snmp-server enable port-traps mac-notification 179
- snmp-server enable traps 176
- snmp-server engine-id 181
- snmp-server group 182
- snmp-server host 177
- snmp-server location 175
- snmp-server notify-filter 190
- snmp-server user 183
- snmp-server view 185
- sntp client 142
- sntp poll 143
- sntp server 144
- spanning-tree 466
- spanning-tree bpdu-filter 477
- spanning-tree bpdu-guard 478
- spanning-tree cisco-prestandard 467
- spanning-tree cost 479
- spanning-tree edge-port 480
- spanning-tree forward-time 467
- spanning-tree hello-time 468
- spanning-tree link-type 481
- spanning-tree loopback-detection 481
- spanning-tree loopback-detection action 482
- spanning-tree loopback-detection release 489
- spanning-tree loopback-detection release-mode 483
- spanning-tree loopback-detection trap 484
- spanning-tree max-age 469
- spanning-tree mode 469
- spanning-tree mst configuration 472
- spanning-tree mst cost 484
- spanning-tree mst port-priority 485
- spanning-tree pathcost method 471
- spanning-tree port-bpdu-flooding 485
- spanning-tree protocol-migration 490
- spanning-tree root-guard 487
- spanning-tree spanning-disabled 488
- spanning-tree system-bpdu-flooding 472
- spanning-tree tc-prop-stop 488
- spanning-tree transmission-limit 473
- speed 127
- speed-duplex 384
- stopbits 127
- subnet-vlan 530
- switchport acceptable-frame-types 505
- switchport allowed vlan 506
- switchport dot1q-tunnel mode 517
- switchport dot1q-tunnel service match cvid 518
- switchport forbidden vlan 498
- switchport gvrp 499
- switchport ingress-filtering 507
- switchport l2protocol-tunnel 524
- switchport mode 508
- switchport native vlan 509
- switchport packet-rate 437
- switchport priority default 544
- switchport trunk allowed vlan 509
- switchport trunk native vlan 510
- switchport voice vlan 537
- switchport voice vlan priority 537
- switchport voice vlan rule 538
- switchport voice vlan security 539
- tacacs-server host 215
- tacacs-server key 215
- tacacs-server port 216
- tacacs-server retransmit 216
- tacacs-server timeout 217
- terminal 129
- test cable-diagnostics 399
- timeout login response 128
- time-range 155
- traceroute 728
- traceroute6 752
- traffic-segmentation 346
- traffic-segmentation session 347
- traffic-segmentation uplink/downlink 348
- traffic-segmentation uplink-to-uplink 349
Index of CLI Commands

transceiver-monitor 390
transceiver-threshold current 391
transceiver-threshold rx-power 393
transceiver-threshold temperature 394
transceiver-threshold tx-power 395
transceiver-threshold voltage 396
transceiver-threshold-auto 391
upgrade opcode auto 115
upgrade opcode path 117
upgrade opcode reload 118
username 205
vlan 502
vlan database 502

vlan-trunking 511
voice vlan 534
voice vlan aging 535
voice vlan mac-address 536
watchdog software 107
web-auth 293
web-auth login-attempts 291
web-auth quiet-period 292
web-auth re-authenticate (IP) 294
web-auth re-authenticate (Port) 294
web-auth session-timeout 292
web-auth system-auth-control 293
whichboot 115
Index

Numerics
802.1Q tunnel 514
   access 517
      configuration, guidelines 514
      configuration, limitations 515
     CVID to SVID map 518
    ethernet type 516
      mode selection 517
     status, configuring 515
    TPID 516
uplink 517
802.1X
   authenticator, configuring 247–253
      global settings 245–247
      port authentication 244, 247
     port authentication accounting 225
      supplicant, configuring 254–257

A
AAA
   accounting 802.1X port settings 225
   accounting exec command privileges 220, 225
   accounting exec settings 226
   accounting summary 228
   accounting update 221
   accounting, configuring 218
   authorization & accounting 218
   authorization command settings 222
   authorization commands, CLI 222
   authorization exec settings 223, 227
   authorization method 227
   authorization service 222
   authorization settings 223
   authorization summary 228
   authorization, cli privilege level 222
   RADIUS group settings 224
   TACACS+ group settings 224
acceptable frame type 505
Access Control List  See ACL
ACL 351
   ARP 370
      binding to a port 356
IPv4 Extended 351, 354, 358
IPv4 Standard 351, 353, 358
IPv6 Extended 358, 360
   IPv6 Standard 358, 359
MAC 364
      time range 155
address table 459
      aging time 459
      aging time, displaying 462
      aging time, setting 459
administrative users, displaying 105
ARP
   ACL 333
      configuration 731
      proxy 732
   ARP inspection 331
      ACL filter 333
      additional validation criteria 335
   ARP ACL 370
      enabling globally 332
      enabling per VLAN 336
trusted ports 337
ARP statistics 727
ATC 149, 438, 761
   control response 443
   functional limitations 441
   limiting traffic rates 440
   shutting down a port 441
   thresholds 444, 445
   timers 441, 442
   usage 440
authentication
   MAC address authentication 277, 285
   MAC, configuring ports 277
   network access 277, 285
   public key 236
   web 293
   web authentication port information, displaying 295
   web authentication, configuring ports 293
   web authentication, re-authenticating address 294
   web authentication, re-authenticating ports 294
   web, configuring 293
Automatic Traffic Control  See ATC

B
BOOTP 724
BPDu
   filter 477
flooding when STA disabled on VLAN 486
flooding when STA globally disabled 472
guard 478
ignoring superior BPDUs 487
selecting protocol based on message format 490
shut down port on receipt 478
bridge extension capabilities, displaying 499
broadcast storm, threshold 437

C

cable diagnostics 399
CDP 699
  enabling for interfaces 702
  enabling globally 700
  hold time 700
  message attributes 699
  transmission interval 701
  version 701
Cisco Discovery Protocol See CDP
class map
  description 555
  DiffServ 554
CLI
  command modes 82
  showing commands 80
clustering switches, management access 159
command line interface See CLI
committed burst size, QoS policy 559, 561, 563
committed information rate, QoS policy 559, 561, 563
community string 61, 173
configuration file, DHCP download reference 69
configuration files, restoring defaults 108
configuration settings
  restoring 65, 108, 110
  saving 65, 108, 110
console port, required connections 52
CoS 550
  configuring 541
  default mapping to internal values 547
  enabling 550
  layer 3/4 priorities 546
  priorities, mapping to internal values 546
  queue mapping 549
  queue mode 542
  queue weights, assigning 543
CoS/CFI to PHB/drop precedence 546
CPU
  status 100
  utilization, setting trap 192
  utilization, showing 100
CVLAN to SPVLAN map 518

D

Daylight Savings Time See summer time
default IPv4 gateway, configuration 726
default IPv6 gateway, configuration 735
default priority, ingress port 544
DHCP 724
  class identifier 714
  client 713, 724
  client identifier 714
  dynamic configuration 58
  relay 719
  relay service, enabling 721
DHCP snooping 296
  enabling 297
  global configuration 297
  information option policy 302
  policy selection 302
  specifying trusted interfaces 306
  subtype field 300
  verifying MAC addresses 303
  VLAN configuration 304
DHCPv4 snooping
  circuit ID, setting 305
  information option 299, 301
  information option, enabling 299, 301
  information option, remote ID 299
  remote ID 301
  sub-length field 300
  sub-option format 300
  sub-type and sub-length, disabling 300
  subtype field 300
DHCPv6 snooping 309
  enabling 310
  global configuration 310
  remote id policy, option 37 313
  remote ID, option 37 312
  specifying trusted interfaces 315
  VLAN configuration 314
DiffServ 553
  binding policy to interface 568
  class map 554, 558
  class map, description 555
  classifying QoS traffic 556
  color aware, srTCM 561
  color aware, trTCM 563
  color blind, srTCM 561
  color blind, trTCM 563
  committed burst size 559, 561, 563
  committed information rate 559, 561, 563
  configuring 553
  conforming traffic, configuring response 559, 561, 563
  description 555
  excess burst size 561
Index

metering, configuring 559
peak burst size 563
peak information rate 563
policy map 557
policy map, description 555
QoS policy 557
service policy 568
setting CoS for matching packets 565
setting IP DSCP for matching packets 566
setting PHB for matching packets 567
single-rate, three-color meter 561
stTCM metering 561
traffic between CIR and BE, configuring response 561
traffic between CIR and PIR, configuring response 563
trTCM metering 563
two-rate, three-color meter 563
violating traffic, configuring response 559, 561, 563

DNS
default domain name 707
displaying the cache 711
domain name list 708
enabling lookup 706
name server list 708
static entries, IPv4 708
static entries, IPv6 709

Domain Name Service  See DNS

DoS protection 340
downloading software 110
automatically 115
using FTP or TFTP 110
drop precedence
CoS priority mapping 546
DSCP ingress map 548

DSA encryption 240
DSCP 550
enabling 550
mapping to internal values 548
DSCP ingress map, drop precedence 548
DSCP to PHB/drop precedence 548
dynamic addresses
clearing 461
displaying 461

Dynamic Host Configuration Protocol  See DHCP
dynamic QoS assignment 280
dynamic VLAN assignment 281

e
edge port, STA 480
cryptograph
DSA 240
RSA 240
engine ID 181
event logging 131
excess burst size, QoS policy 561, 563
exec command privileges, accounting 220, 225
exec settings
accounting 226
authorization 223, 227

F
FIB, description 773
firmware
displaying version 106
upgrading 110
upgrading automatically 115
upgrading with FTP or TFTP 110
version, displaying 106
forwarding information base  See FIB

g
gateway, IPv4 default 726
gateway, IPv6 default 735
general security measures 271
GVRP
enabling 496
global setting 496
interface configuration 499

H
hardware version, displaying 106
HTTP, web server 230
HTTPS 231
configuring 231
replacing SSL certificate 110
secure-site certificate 110
UDP port, configuring 230
HTTPS, secure server 231

I
IEEE 802.1D 469
IEEE 802.1s 469
IEEE 802.1w 469
IEEE 802.1x 244, 247
IGMP
filter profiles, binding to interface 601
filter profiles, configuration 597
filter, interface configuration 601–602
filter, parameters 597–602
filtering & throttling 596
filtering & throttling, enabling 597
filtering & throttling, interface configuration 599–??
filtering & throttling, status 597
filtering, configuring profile 598
filtering, creating profile 597
filtering, group range 598

Index

filtering, interface settings 601–602
  groups, displaying 590
Layer 2 572
query 575
query, RADIUS authentication 599
services, displaying 590
snooping 572
snooping & query, parameters 572
snooping, configuring 572
snooping, enabling 573
snooping, immediate leave 582
IGMP snooping
  configuring 572
  enabling per interface 573
  forwarding entries 590
  immediate leave, status 582
  interface attached to multicast router 591, 595
  last member query count 583
  last member query interval 583
  proxy query address 585
  proxy query interval 586
  proxy query response interval 587
  proxy reporting 574, 611
  querier, enabling 575
  router port expire time 576
  static host interface 588
  static multicast routing 595
  static port assignment 588
  static router interface 595
  static router port, configuring 595
  statistics, displaying 592, 620
  TCN flood 577
  unregistered data flooding 579
  version exclusive 581
  with proxy reporting 574, 611
  immediate leave, IGMP snooping 582
  immediate leave, MLD snooping 615
  importing user public keys 110
ingress filtering 507
IP address
  BOOTP/DHCP 715
  setting 723
IP filter, for management access 260
IP routing 771
  unicast protocols 771
IP source guard
  configuring static entries 319
  setting filter criteria 321
  setting maximum bindings 323, 324
IP statistics 727

IPv4 address
  BOOTP/DHCP 724
  dynamic configuration 58
  manual configuration 55
  setting 55, 724
IPv6
  displaying neighbors 760
  duplicate address detection 755, 760
  enabling 742
  MTU 743
  router advertisements, blocking 757
  statistics 747
IPv6 address
  dynamic configuration (global unicast) 59, 737
  dynamic configuration (link-local) 59, 742
  EUI format 739
  EUI-64 setting 739
  explicit configuration 742
  global unicast 736
  link-local 737, 741
  manual configuration (global unicast) 56, 736
  manual configuration (link-local) 56, 741
  setting 55, 736
IPv6 source guard
  configuring static entries 326
  setting maximum bindings 329

J
  jumbo frame 107

K
  key
    private 234
    public 234
    user public, importing 110
  key pair
    host 234
    host, generating 240

L
  LACP
    configuration 403
    group attributes, configuring 410
    group members, configuring 406–410
    local parameters 412
    partner parameters 412
    protocol message statistics 412
    protocol parameters 403
    timeout, for LACPDU 411
  last member query count, IGMP snooping 583
  last member query interval, IGMP snooping 583
  layer 2, protocol tunnel 524
license information 781
Link Layer Discovery Protocol See LLDP
link type, STA 481
LLDP 673
device statistics details, displaying 695
device statistics, displaying 695
display device information 694
displaying remote information 694
interface attributes, configuring 679–690
local device information, displaying 693
message attributes 673
message statistics 695
remote information, displaying 694
remote port information, displaying 694
timing attributes, configuring 675–678
TLV, 802.1 682–683
TLV, 802.3 684–685
TLV, basic 679–681
TLV, management address 679
TLV, port description 680
TLV, system capabilities 680
TLV, system description 681
TLV, system name 681
LLDP-MED 673
notification, status 688
TLV 673
TLV, extended PoE 688
TLV, inventory 689
TLV, location 686, 689
TLV, MED capabilities 690
TLV, network policy 690
TLV, PoE 688
local engine ID 181
logging
messages, displaying 135
syslog traps 134
to syslog servers 133
logon authentication 203
encryption keys 212, 215
RADIUS client 210
RADIUS server 210
sequence 208, 209
settings 209
TACACS+ client 214
TACACS+ server 214
logon authentication, settings 210, 214
loopback detection
non-STA 453
loopback detection, STA 481

MAC address, mirroring 425
management access, filtering per address 260
management access, IP filter 260
matching class settings, classifying QoS traffic 556
media-type 382
memory
status 100
utilization, showing 100
memory utilization, setting trap 192
mirror port
configuring 425
configuring local traffic 425
configuring remote traffic 428
mirror trunk
configuring 425
configuring local traffic 425
MLD
filter profiles, configuration 622
filtering & throttling 621
filtering & throttling, configuring profile 623
filtering & throttling, creating profile 622
filtering & throttling, enabling 622
filtering & throttling, interface configuration 624–626
filtering & throttling, status 622
MLD snooping 608
configuring 608
enabling 609
immediate leave 615
immediate leave, status 615
multicast static router port 615
querier 609
querier, enabling 609
query interval 610
query, maximum response time 611
robustness value 612
static port assignment 616
static router port 615
unknown multicast, handling 613
version 614
MSTP 469
global settings, configuring 465
global settings, displaying 491
interface settings, configuring 466
interface settings, displaying 490
max hop count 474
path cost 484
region name 476
region revision 476
MTU for IPv6 743
multicast filtering 571
enabling IGMP snooping 573
enabling IGMP snooping per interface 573
enabling MLD snooping 609
router configuration 595

M
MAC address authentication 277
ports, configuring 277, 285
reauthentication 279
multicast groups 590
  static 588, 590
Multicast Listener Discovery See MLD snooping
multicast router discovery 584
multicast router port, displaying 591
multicast services
  configuring 588
  displaying 590
multicast static router port 595
  configuring 595
  configuring for MLD snooping 615
multicast storm, threshold 437
multicast, filtering and throttling 597, 622
MVR
  assigning static multicast groups 634, 642
  configuring 630, 639
  interface status, configuring 640–642
  interface status, displaying 644
  IP for control packets sent upstream 638
  proxy switching 636
  receiver groups, displaying 646
  robust value for proxy switching 637
  setting interface type 641
  setting multicast domain 632
  setting multicast groups 631, 634
  setting multicast priority 633, 656
  specifying a domain 632
  specifying a VLAN 631, 639
  specifying priority 633, 656
  static binding 634, 642
  static binding, group to port 642
  statistics, displaying 648
  using immediate leave 640
MVR6
  assigning static multicast groups 657, 664
  configuring 654, 661
  interface status, configuring 662–664
  interface status, displaying 668
  IP for control packets sent upstream 661
  proxy switching 658
  receiver groups, displaying 669
  robust value for proxy switching 659
  setting interface type 663
  setting multicast domain 655
  setting multicast groups 657
  setting multicast priority 656
  specifying a domain 655
  specifying a VLAN 661
  specifying priority 656
  static binding 657, 664
  static binding, group to port 664
  statistics, displaying 671
  using immediate leave 662

N
ND snooping
  automatic validation 764–765
  enabling 762
  max bindings 766
  trusted interface 767
Neighbor Discovery Snooping See ND snooping
network access
  authentication 277
  dynamic QoS assignment 280
  dynamic VLAN assignment 281
  guest VLAN 282
  MAC address filter 278
  port configuration 285
  reauthentication 279
  secure MAC information 289, 290
NTP
  authentication keys, specifying 146
  client, enabling 147
  specifying servers 147
NTP, setting the system clock 145–148
P
password, line 124
passwords 53, 204
  administrator setting 205
path cost 479
  method 471
  STA 471, 479
peak burst size, QoS policy 563
peak information rate, QoS policy 563
per-hop behavior, DSCP ingress map 548
policy map
  description 555
  DiffServ 557
port authentication 244, 247
port power
  displaying status 423
  inline 419
  inline status 423
  maximum allocation 420
  priority 421
  time range 155, 422
port priority
  configuring 541
  default ingress 544
  STA 485, 486
port security, configuring 272
ports
  autonegotiation 383
  broadcast storm threshold 437
  capabilities 379
  configuring 377
duplex mode 384
flow control 381
forced selection of media type 382
forced selection on combo ports 382
mirroring 425
mirroring local traffic 425
mirroring remote traffic 428
multicast storm threshold 437
speed 384
statistics 386
unknown unicast storm threshold 437
power budgets
port 420
port priority 421
power savings
configuring 401
enabling per port 401
PPPoE 262–269
priority, default port ingress 544
private key 234
privilege level, defining per command 207
problems, troubleshooting 779
protocol migration 490
protocol tunnel, layer 2 524
protocol VLANs 525
configuring 525
configuring groups 526
configuring interfaces 527
group configuration 526
interface configuration 527
proxy ARP 732
proxy query address, IGMP snooping 585
proxy query interval, IGMP snooping 586
proxy query response interval, IGMP snooping 587
proxy reporting, IGMP snooping 574, 611
public key 234
PVID, port native VLAN 509

Q
QoS 553
configuration guidelines 554
configuring 553
CoS/CFI to PHB/drop precedence 546
DSCP to PHB/drop precedence 548
dynamic assignment 280
matching class settings 556
PHB to queue 549
selecting DSCP, CoS 550
QoS policy
committed burst size 559, 561, 563
excess burst size 561
peak burst size 561
srTCM 561
srTCM police meter 561
trTCM 563
trTCM police meter 563
QoS policy, committed information rate 559, 561, 563
QoS policy, peak information rate 563
queue mode, setting 542
queue weight, assigning to CoS 543

R
RADIUS
logon authentication 210
settings 210
rate limit
port 436
setting 435
remote engine ID 181
remote logging 134
Remote Monitoring  See RMON
rename, DiffServ 557
restarting the system 90, 94, 95
at scheduled times 90
RMON 195
alarm, displaying settings 200
alarm, setting thresholds 196
commands 195
event settings, displaying 200
response to alarm setting 197
statistics history, collection 198
statistics history, displaying 200
statistics, collection 199
statistics, displaying 201
root guard 487
routing information base, description 773
routing table, displaying 773
RSA encryption 240
RSTP 469
global settings, configuring 469
global settings, displaying 490
interface settings, configuring 477–488
interface settings, displaying 490
running configuration files, displaying 101

S
secure shell 234
configuration 235
security, general measures 271
serial port, configuring 120
SMTP
event handling 138
sending log events 138
SNMP 171
community string 173
enabling traps 176
enabling traps, mac-address changes 179
Index

filtering IP addresses 260
  global settings, configuring 173
mac address traps 176, 179
  trap manager 177
SNMPv3 181–183
  engine ID 181
  engine identifier, local 181
  engine identifier, remote 181
groups 182
local users, configuring 183
remote users, configuring 183
user configuration 183
views 185
SNTP
  setting the system clock 142–144
  specifying servers 144
software
  displaying version 106
  downloading 110
  version, displaying 106
srTCM
  police meter 561
  QoS policy 561
SSH 234
  authentication retries 237
  configuring 235
  downloading public keys for clients 110
  generating host key pair 240
  server, configuring 238
timeout 239
ST
  system clock
    setting 141
    setting manually 153
    setting the time zone 153
    setting with NTP 145–148
    setting with SNTP 142–144
    summer time 149–151
system logs 133
system software, downloading from server 110

T
TACACS+
  logon authentication 214
  settings 214
TCN
  flood 577
  general query solicitation 578
Telnet
  configuring 232
  server, enabling 234
telnet connection, configuring 120
terminal, configuration settings 129
TFTP
  retry count 118
  timeout 119
time range, ACL 155
time range, PoE 155, 422
time zone, setting 153
time, setting 141
TPID 516
traffic segmentation 346
  assigning ports 348
  enabling 346
sessions, assigning ports 348
sessions, creating 347
transceiver thresholds
displaying 398
trap manager 62, 177
troubleshooting 779, 781
trTCM
police meter 563
QoS policy 563
trunk
configuration 403
LACP 403, 406
load balancing 404
static 406
trunks
mirroring 425
mirroring local traffic 425
tunneling unknown VLANs, VLAN trunking 511

U
unicast routing 771
unknown unicast storm, threshold 437
unregistered data flooding, IGMP snooping 579
upgrading software 110, 115
user account 204, 205
user password 204, 205

V
VLAN trunking 511
VLANs 495–539
  802.1Q tunnel mode 517
  acceptable frame type 505
  adding static members 506
  basic information, displaying 499
  configuring port members, by interface 505–509
  creating 502
displaying port members 513
dynamic assignment 281
egress mode 508
ingress filtering 507
interface configuration 505–511
IP subnet-based 529
MAC-based 531
mirroring 425
port members, displaying 513
protocol 525
protocol, configuring 525
protocol, configuring groups 526
protocol, configuring interfaces 527
protocol, group configuration 526
protocol, interface configuration 527
PVID 509
tunneling unknown groups 511
voice 533
voice VLANs 533
detecting VoIP devices 534
enabling for ports 537–539
identifying client devices 536
VoIP traffic 533
  ports, configuring 537–539
telephony OUI, configuring 536
voice VLAN, configuring 533
VoIP, detecting devices 538

W
web authentication 293
  address, re-authenticating 294
  configuring 293
  configuring ports 293
  port information, displaying 295
  ports, configuring 293
  ports, re-authenticating 294