



ECS4810-12M Layer 2  
Gigabit Ethernet Switch

Software Release v1.2.0.1

CLI Reference Guide

# CLI Reference Guide

---

## **ECS4810-12M Gigabit Ethernet Switch**

Layer 2 Gigabit Ethernet Switch  
with 12 Gigabit Combination Ports (RJ-45/SFP)

---

# How to Use This 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 or information about the web browser management interface refer to the *Web Management Guide*.

The guide includes these sections:

- ◆ Section I "[Getting Started](#)" — Includes an introduction to switch management, and the basic settings required to access the management interface.
- ◆ Section II "[Command Line Interface](#)" — Includes all management options available through the web browser interface.
- ◆ Section III "[Appendices](#)" — Includes information on troubleshooting switch management access.

**Related Documentation** This guide focuses on switch software configuration through the command line interface.



**Note:** For a description of how to initialize the switch for management access via the CLI, web interface or SNMP, refer to "[Initial Switch Configuration](#)" on page 49 in this guide.

---

For information on how to manage the switch through the web browser, see the following guide:

*Web Management 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*

**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.

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

| <b>Revision</b> | <b>Date</b> | <b>Change Description</b>  |
|-----------------|-------------|--|
| v1.2.0.1        | 5/2014      | <b>New:</b> <ul style="list-style-type: none"><li>♦ "show process cpu guard" on page 105</li><li>♦ "snmp-server enable port-traps mac-notification" on page 184</li><li>♦ "show snmp-server enable port-traps" on page 184</li><li>♦ "process cpu guard" on page 198</li><li>♦ "telnet (client)" on page 241</li><li>♦ "ip dhcp snooping information option encode no-subtype" on page 308</li><li>♦ "ip dhcp snooping information option remote-id" on page 309</li><li>♦ "transceiver-threshold-auto" on page 391</li><li>♦ "ipv6 mld snooping proxy-reporting" on page 643</li><li>♦ "ipv6 mld snooping unsolicited-report-interval" on page 647</li><li>♦ "show ipv6 mld snooping statistics" on page 654</li><li>♦ "ip dhcp dynamic-provision" on page 800</li><li>♦ "ipv6 hop-limit" on page 843</li></ul> |

| <i>Revision</i> | <i>Date</i> | <i>Change Description</i>  |
|-----------------|-------------|--|
| v1.2.0.1        | 5/2014      | <p><b>Updated:</b></p> <ul style="list-style-type: none"> <li>♦ "snmp-server enable traps" on page 180</li> <li>♦ "snmp-server user" on page 187</li> <li>♦ "radius-server key" on page 222</li> <li>♦ "ip http secure-port" on page 237</li> <li>♦ "dot1x default" on page 253</li> <li>♦ "network-access guest-vlan" on page 289</li> <li>♦ "ip source-guard binding" on page 317</li> <li>♦ "dos-protection echo-charge" on page 332</li> <li>♦ "permit, deny (Extended IPv6 ACL)" on page 353</li> <li>♦ "clear access-list hardware counters" on page 365</li> <li>♦ "interface" on page 370</li> <li>♦ "show interfaces brief" on page 380</li> <li>♦ "transceiver-threshold current" on page 392</li> <li>♦ "lACP admin-key (Ethernet Interface)" on page 408</li> <li>♦ "lACP system-priority" on page 410</li> <li>♦ "auto-traffic-control control-release" on page 439</li> <li>♦ "clear mac-address-table dynamic" on page 455</li> <li>♦ "spanning-tree bpdu-filter" on page 471</li> <li>♦ "spanning-tree port-priority" on page 481</li> <li>♦ "switchport allowed vlan" on page 531</li> <li>♦ "voice vlan aging" on page 560</li> <li>♦ "show voice vlan" on page 565</li> <li>♦ "show policy-map" on page 601</li> <li>♦ "show policy-map interface" on page 602</li> <li>♦ "show ipv6 mld snooping" on page 651</li> <li>♦ "show ipv6 mld snooping group source-list" on page 652</li> <li>♦ "show mvr6 statistics" on page 704</li> <li>♦ "ma index name" on page 744</li> <li>♦ "ip domain-list" on page 789</li> <li>♦ "ip dhcp client class-id" on page 801</li> <li>♦ "ipv6 dhcp client rapid-commit vlan" on page 804</li> <li>♦ "show ipv6 dhcp vlan" on page 806</li> <li>♦ "ip address" on page 814</li> <li>♦ "ipv6 nd reachable-time" on page 847</li> </ul> <p><b>Removed:</b></p> <ul style="list-style-type: none"> <li>♦ "ip igmp query-drop"</li> <li>♦ "show ip igmp query-drop"</li> </ul> |

| <b>Revision</b> | <b>Date</b> | <b>Change Description</b>   |
|-----------------|-------------|---|
| v1.1.4.11       | 5/2014      | <b>New:</b> <ul style="list-style-type: none"><li>♦ "clock summer-time (date)" on page 739</li><li>♦ "clock summer-time (predefined)" on page 741</li><li>♦ "clock summer-time (recurring)" on page 742</li><li>♦ "Loopback Detection Commands" on page 1021</li><li>♦ "mvr6 priority" on page 1256</li></ul> <b>Updated:</b> <ul style="list-style-type: none"><li>♦ "ip dhcp client class-id" on page 1362</li></ul>  |
| v1.1.4.9        | 2/2014      | <b>Updated:</b> <ul style="list-style-type: none"><li>♦ "spanning-tree bpdu-filter" on page 467</li></ul>   |
| v1.1.4.8        | 12/2013     | <b>New:</b> <ul style="list-style-type: none"><li>♦ "show alarm" on page 694</li><li>♦ "show alarm-status" on page 695</li><li>♦ "show watchdog" on page 702</li><li>♦ "watchdog software" on page 702</li><li>♦ "upgrade opcode reload" on page 713</li><li>♦ "show upgrade" on page 713</li><li>♦ "TFTP Configuration Commands" on page 713</li><li>♦ "terminal" on page 724</li><li>♦ "Synchronous Ethernet" on page 748</li><li>♦ "memory" on page 784</li><li>♦ "process cpu" on page 785</li><li>♦ "PPPoE Intermediate Agent" on page 854</li><li>♦ "ip dhcp snooping information option circuit-id" on page 895</li><li>♦ "clear ip dhcp snooping binding" on page 897</li><li>♦ "clear access-list hardware counters" on page 946</li><li>♦ "discard" on page 953</li><li>♦ "show discard" on page 959</li><li>♦ "transceiver-monitor" on page 967</li><li>♦ "show interfaces transceiver-threshold" on page 974</li><li>♦ "lACP timeout" on page 987</li><li>♦ "mep-monitor" on page 1074</li><li>♦ "non-revertive" on page 1077</li><li>♦ "raps-def-mac" on page 1082</li><li>♦ "raps-without-vc" on page 1082</li><li>♦ "rpl neighbor" on page 1085</li><li>♦ "version" on page 1087</li><li>♦ "erps clear" on page 1089</li><li>♦ "erps forced-switch" on page 1089</li><li>♦ "erps manual-switch" on page 1091</li><li>♦ "non-erps-dev-protect" on page 1076</li></ul> |

| <i>Revision</i> | <i>Date</i> | <i>Change Description</i>   |
|-----------------|-------------|---|
| v1.1.4.8        | 12/2013     | <p><b>New</b> (continued):</p> <ul style="list-style-type: none"> <li>◆ "clear erps statistics" on page 1088</li> <li>◆ "Configuring VLAN Translation" on page 1125</li> <li>◆ "bundle" on page 1163</li> <li>◆ "clear ip igmp snooping statistics" on page 1195</li> <li>◆ "ip igmp authentication" on page 1204</li> <li>◆ "ip igmp query-drop" on page 1208</li> <li>◆ "ip multicast-data-drop" on page 1208</li> <li>◆ "show ip igmp authentication" on page 1209</li> <li>◆ "show ip i"show ip multicast-data-drop" on page 1212</li> <li>◆ "show ip igmp query-drop" on page 1211</li> <li>◆ "show ip multicast-data-drop" on page 1212</li> <li>◆ "MLD Snooping" on page 1213</li> <li>◆ "MLD Filtering and Throttling" on page 1223</li> <li>◆ "mvr" on page 1233</li> <li>◆ "mvr proxy-query-interval" on page 1236</li> <li>◆ "mvr source-port-mode dynamic" on page 1239</li> <li>◆ "clear mrv groups dynamic" on page 1244</li> <li>◆ "clear mrv statistics" on page 1244</li> <li>◆ "mvr6 proxy-query-interval" on page 1258</li> <li>◆ "mvr6 source-port-mode dynamic" on page 1260</li> <li>◆ "clear mvr6 groups dynamic" on page 1265</li> <li>◆ "clear mvr6 statistics" on page 1266</li> <li>◆ "clear efm oam event-log" on page 1344</li> <li>◆ "ipv6 dhcp client rapid-commit vlan" on page 1364</li> <li>◆ "DHCP Relay Option 82" on page 1367</li> <li>◆ "traceroute6" on page 1402</li> <li>◆ "ipv6 nd rguard" on page 1405</li> <li>◆ "show ipv6 nd rguard" on page 1407</li> <li>◆ "ND Snooping" on page 1409</li> <li>◆ "delete" on page 708</li> <li>◆ "logging host" on page 728</li> <li>◆ "Flow Sampling Commands" on page 795</li> <li>◆ "permit, deny (Extended IPv4 ACL)" on page 928</li> <li>◆ "ip access-group" on page 930</li> <li>◆ "ipv6 access-group" on page 936</li> <li>◆ "mac access-group" on page 941</li> <li>◆ "show access-list" on page 947</li> <li>◆ "transceiver-threshold current" on page 968</li> <li>◆ "transceiver-threshold rx-power" on page 969</li> <li>◆ "transceiver-threshold temperature" on page 970</li> <li>◆ "transceiver-threshold tx-power" on page 971</li> </ul> |

| <i>Revision</i> | <i>Date</i> | <i>Change Description</i>  |
|-----------------|-------------|--|
|                 |             | <b>Updated</b> (continued): <ul style="list-style-type: none"><li>♦ "transceiver-threshold voltage" on page 972</li><li>♦ "port monitor" on page 993</li><li>♦ "show spanning-tree" on page 1064</li><li>♦ "erps domain" on page 1069</li><li>♦ "ring-port" on page 1084</li><li>♦ "show erps" on page 1093</li><li>♦ "switchport dot1q-tunnel service match cvid" on page 1117</li><li>♦ "protocol-vlan protocol-group (Configuring Interfaces)" on page 1129</li><li>♦ "match" on page 1160</li><li>♦ "show mvr statistics" on page 1249"ethernet cfm cc ma interval" on page 1317</li><li>♦ "ethernet cfm loopback" on page 1331</li><li>♦ "ipv6 dhcp restart client vlan" on page 1364</li><li>♦ "ip address" on page 1374</li></ul> |
| v1.0.6.0        | 6/2011      | Initial release  |

---

# Contents

|                              |           |
|------------------------------|-----------|
| <b>How to Use This Guide</b> | <b>3</b>  |
| <b>Contents</b>              | <b>9</b>  |
| <b>Figures</b>               | <b>39</b> |
| <b>Tables</b>                | <b>41</b> |

---

|                  |  |           |
|------------------|--|-----------|
| <b>Section I</b> | <b>Getting Started</b>                                       | <b>47</b> |
|                  | <b>1 Initial Switch Configuration</b>                        | <b>49</b> |
|                  | Connecting to the Switch                                     | 49        |
|                  | Configuration Options  | 49        |
|                  | Required Connections   | 50        |
|                  | Remote Connections   | 51        |
|                  | Basic Configuration  | 52        |
|                  | Console Connection   | 52        |
|                  | Setting Passwords  | 52        |
|                  | Setting an IP Address  | 53        |
|                  | Downloading a Configuration File Referenced by a DHCP Server | 59        |
|                  | Enabling SNMP Management Access                              | 61        |
|                  | Managing System Files  | 63        |
|                  | Saving or Restoring Configuration Settings                   | 64        |

---

|                   |   |           |
|-------------------|---|-----------|
| <b>Section II</b> | <b>Command Line Interface</b>             | <b>67</b> |
|                   | <b>2 Using the Command Line Interface</b> | <b>69</b> |
|                   | Accessing the CLI                         | 69        |
|                   | Console Connection                        | 69        |
|                   | Telnet Connection                         | 70        |

|                                     |           |
|-------------------------------------|-----------|
| Entering Commands                   | 71        |
| Keywords and Arguments              | 71        |
| Minimum Abbreviation                | 71        |
| Command Completion                  | 71        |
| Getting Help on Commands            | 72        |
| Partial Keyword Lookup              | 74        |
| Negating the Effect of Commands     | 74        |
| Using Command History               | 74        |
| Understanding Command Modes         | 74        |
| Exec Commands                       | 75        |
| Configuration Commands              | 76        |
| Command Line Processing             | 78        |
| Showing Status Information          | 78        |
| Output Modifiers                    | 79        |
| CLI Command Groups                  | 79        |
| <b>3 General Commands</b>           | <b>83</b> |
| prompt                              | 83        |
| reload (Global Configuration)       | 84        |
| enable                              | 85        |
| quit                                | 86        |
| show history                        | 86        |
| configure                           | 87        |
| disable                             | 88        |
| reload (Privileged Exec)            | 88        |
| show reload                         | 89        |
| end                                 | 89        |
| exit                                | 89        |
| <b>4 System Management Commands</b> | <b>91</b> |
| Device Designation                  | 91        |
| hostname                            | 92        |
| Banner Information                  | 92        |
| banner configure                    | 93        |
| banner configure company            | 94        |
| banner configure dc-power-info      | 95        |

|                                     |     |
|-------------------------------------|-----|
| banner configure department         | 95  |
| banner configure equipment-info     | 96  |
| banner configure equipment-location | 97  |
| banner configure ip-lan             | 97  |
| banner configure lp-number          | 98  |
| banner configure manager-info       | 99  |
| banner configure mux                | 99  |
| banner configure note               | 100 |
| show banner                         | 101 |
| System Status                       | 101 |
| show access-list tcam-utilization   | 102 |
| show alarm                          | 102 |
| show alarm-status                   | 103 |
| show memory                         | 104 |
| show process cpu                    | 104 |
| show process cpu guard              | 105 |
| show running-config                 | 106 |
| show startup-config                 | 108 |
| show system                         | 108 |
| show tech-support                   | 109 |
| show users                          | 110 |
| show version                        | 110 |
| show watchdog                       | 111 |
| watchdog software                   | 111 |
| Frame Size                          | 112 |
| jumbo frame                         | 112 |
| File Management                     | 113 |
| General Commands                    | 114 |
| boot system                         | 114 |
| copy                                | 115 |
| delete                              | 118 |
| dir                                 | 119 |
| whichboot                           | 120 |
| Automatic Code Upgrade Commands     | 120 |
| upgrade opcode auto                 | 120 |

|                                    |     |
|------------------------------------|-----|
| upgrade opcode path                | 121 |
| upgrade opcode reload              | 122 |
| show upgrade                       | 123 |
| TFTP Configuration Commands        | 123 |
| ip tftp retry                      | 123 |
| ip tftp timeout                    | 124 |
| Line                               | 125 |
| line                               | 125 |
| databits                           | 126 |
| exec-timeout                       | 127 |
| login                              | 128 |
| parity                             | 129 |
| password                           | 129 |
| password-thresh                    | 130 |
| silent-time                        | 131 |
| speed                              | 131 |
| stopbits                           | 132 |
| timeout login response             | 133 |
| disconnect                         | 133 |
| terminal                           | 134 |
| show line                          | 135 |
| Event Logging                      | 136 |
| logging facility                   | 136 |
| logging history                    | 137 |
| logging host                       | 138 |
| logging on                         | 138 |
| logging trap                       | 139 |
| clear log                          | 140 |
| show log                           | 140 |
| show logging                       | 141 |
| SMTP Alerts                        | 142 |
| logging sendmail                   | 143 |
| logging sendmail host              | 143 |
| logging sendmail level             | 144 |
| logging sendmail destination-email | 145 |

|                                    |     |
|------------------------------------|-----|
| logging sendmail source-email      | 145 |
| show logging sendmail              | 146 |
| Time                               | 146 |
| SNTP Commands                      | 147 |
| sntp client                        | 147 |
| sntp poll                          | 148 |
| sntp server                        | 148 |
| show sntp                          | 149 |
| Manual Configuration Commands      | 149 |
| clock summer-time (date)           | 149 |
| clock summer-time (predefined)     | 151 |
| clock summer-time (recurring)      | 152 |
| clock timezone                     | 153 |
| calendar set                       | 154 |
| show calendar                      | 155 |
| Time Range                         | 155 |
| time-range                         | 155 |
| absolute                           | 156 |
| periodic                           | 157 |
| show time-range                    | 158 |
| Synchronous Ethernet               | 158 |
| synce                              | 159 |
| synce ethernet                     | 160 |
| synce ethernet clock-source        | 161 |
| synce auto-clock-source-selecting  | 162 |
| synce force-clock-source-selecting | 163 |
| synce ssm ethernet                 | 164 |
| synce clk-src-ssm                  | 166 |
| show synce                         | 166 |
| Switch Clustering                  | 168 |
| cluster                            | 169 |
| cluster commander                  | 170 |
| cluster ip-pool                    | 171 |
| cluster member                     | 171 |
| rcommand                           | 172 |

|  |            |
|--|------------|
| show cluster                                   | 172        |
| show cluster members                           | 173        |
| show cluster candidates                        | 173        |
| <b>5 SNMP Commands</b>                         | <b>175</b> |
| General SNMP Commands                          | 177        |
| snmp-server                                    | 177        |
| snmp-server community                          | 178        |
| snmp-server contact                            | 178        |
| snmp-server location                           | 179        |
| show snmp                                      | 179        |
| SNMP Target Host Commands                      | 180        |
| snmp-server enable traps                       | 180        |
| snmp-server host                               | 182        |
| snmp-server enable port-traps mac-notification | 184        |
| show snmp-server enable port-traps             | 184        |
| SNMPv3 Commands                                | 185        |
| snmp-server engine-id                          | 185        |
| snmp-server group                              | 186        |
| snmp-server user                               | 187        |
| snmp-server view                               | 189        |
| show snmp engine-id                            | 190        |
| show snmp group                                | 191        |
| show snmp user                                 | 192        |
| show snmp view                                 | 193        |
| Notification Log Commands                      | 193        |
| nlm  | 193        |
| snmp-server notify-filter                      | 194        |
| show nlm oper-status                           | 195        |
| show snmp notify-filter                        | 196        |
| Additional Trap Commands                       | 196        |
| memory   | 196        |
| process cpu                                    | 197        |
| process cpu guard                              | 198        |

|                                     |            |
|-------------------------------------|------------|
| <b>6 Remote Monitoring Commands</b> | <b>201</b> |
| rmon alarm                          | 202        |
| rmon event                          | 203        |
| rmon collection history             | 204        |
| rmon collection rmon1               | 205        |
| show rmon alarms                    | 206        |
| show rmon events                    | 206        |
| show rmon history                   | 206        |
| show rmon statistics                | 207        |
| <b>7 Flow Sampling Commands</b>     | <b>209</b> |
| sflow owner                         | 209        |
| sflow polling instance              | 211        |
| sflow sampling instance             | 212        |
| show sflow                          | 213        |
| <b>8 Authentication Commands</b>    | <b>215</b> |
| User Accounts                       | 216        |
| enable password                     | 216        |
| username                            | 217        |
| Authentication Sequence             | 218        |
| authentication enable               | 218        |
| authentication login                | 219        |
| RADIUS Client                       | 220        |
| radius-server acct-port             | 220        |
| radius-server auth-port             | 221        |
| radius-server host                  | 221        |
| radius-server key                   | 222        |
| radius-server retransmit            | 223        |
| radius-server timeout               | 223        |
| show radius-server                  | 224        |
| TACACS+ Client                      | 224        |
| tacacs-server host                  | 225        |
| tacacs-server key                   | 225        |
| tacacs-server port                  | 226        |
| tacacs-server retransmit            | 226        |

|                                 |     |
|---------------------------------|-----|
| tacacs-server timeout           | 227 |
| show tacacs-server              | 227 |
| AAA                             | 228 |
| aaa accounting dot1x            | 228 |
| aaa accounting exec             | 229 |
| aaa accounting update           | 230 |
| aaa authorization exec          | 231 |
| aaa group server                | 232 |
| server                          | 232 |
| accounting dot1x                | 233 |
| accounting exec                 | 233 |
| authorization exec              | 234 |
| show accounting                 | 235 |
| Web Server                      | 236 |
| ip http port                    | 236 |
| ip http server                  | 237 |
| ip http secure-port             | 237 |
| ip http secure-server           | 238 |
| Telnet Server                   | 239 |
| ip telnet max-sessions          | 240 |
| ip telnet port                  | 240 |
| ip telnet server                | 241 |
| telnet (client)                 | 241 |
| show ip telnet                  | 242 |
| Secure Shell                    | 242 |
| ip ssh authentication-retries   | 245 |
| ip ssh server                   | 245 |
| ip ssh server-key size          | 246 |
| ip ssh timeout                  | 247 |
| delete public-key               | 247 |
| ip ssh crypto host-key generate | 248 |
| ip ssh crypto zeroize           | 249 |
| ip ssh save host-key            | 249 |
| show ip ssh                     | 250 |
| show public-key                 | 250 |

|   |     |
|---|-----|
| show ssh                                  | 251 |
| 802.1X Port Authentication                | 252 |
| General Commands                          | 253 |
| dot1x default                             | 253 |
| dot1x eapol-pass-through                  | 254 |
| dot1x system-auth-control                 | 254 |
| Authenticator Commands                    | 255 |
| dot1x intrusion-action                    | 255 |
| dot1x max-reauth-req                      | 255 |
| dot1x max-req                             | 256 |
| dot1x operation-mode                      | 256 |
| dot1x port-control                        | 257 |
| dot1x re-authentication                   | 258 |
| dot1x timeout quiet-period                | 258 |
| dot1x timeout re-authperiod               | 259 |
| dot1x timeout supp-timeout                | 259 |
| dot1x timeout tx-period                   | 260 |
| dot1x re-authenticate                     | 261 |
| Supplicant Commands                       | 261 |
| dot1x identity profile                    | 261 |
| dot1x max-start                           | 262 |
| dot1x pae supplicant                      | 262 |
| dot1x timeout auth-period                 | 263 |
| dot1x timeout held-period                 | 264 |
| dot1x timeout start-period                | 264 |
| Information Display Commands              | 265 |
| show dot1x                                | 265 |
| Management IP Filter                      | 268 |
| management                                | 268 |
| show management                           | 269 |
| PPPoE Intermediate Agent                  | 270 |
| pppoe intermediate-agent                  | 270 |
| pppoe intermediate-agent format-type      | 271 |
| pppoe intermediate-agent port-enable      | 272 |
| pppoe intermediate-agent port-format-type | 273 |

|   |            |
|---|------------|
| pppoe intermediate-agent trust              | 274        |
| pppoe intermediate-agent vendor-tag strip   | 274        |
| clear pppoe intermediate-agent statistics   | 275        |
| show pppoe intermediate-agent info          | 275        |
| show pppoe intermediate-agent statistics    | 276        |
| <b>9 General Security Measures</b>          | <b>279</b> |
| Port Security                               | 280        |
| port security                               | 280        |
| show port security                          | 282        |
| Network Access (MAC Address Authentication) | 284        |
| network-access aging                        | 285        |
| network-access mac-filter                   | 286        |
| mac-authentication reauth-time              | 287        |
| network-access dynamic-qos                  | 287        |
| network-access dynamic-vlan                 | 288        |
| network-access guest-vlan                   | 289        |
| network-access link-detection               | 290        |
| network-access link-detection link-down     | 290        |
| network-access link-detection link-up       | 291        |
| network-access link-detection link-up-down  | 291        |
| network-access max-mac-count                | 292        |
| network-access mode mac-authentication      | 293        |
| network-access port-mac-filter              | 294        |
| mac-authentication intrusion-action         | 294        |
| mac-authentication max-mac-count            | 295        |
| clear network-access mac-address-table      | 295        |
| show network-access                         | 296        |
| show network-access mac-address-table       | 297        |
| show network-access mac-filter              | 298        |
| Web Authentication                          | 298        |
| web-auth login-attempts                     | 299        |
| web-auth quiet-period                       | 300        |
| web-auth session-timeout                    | 300        |
| web-auth system-auth-control                | 301        |

|   |     |
|---|-----|
| web-auth  | 301 |
| web-auth re-authenticate (Port)                       | 302 |
| web-auth re-authenticate (IP)                         | 302 |
| show web-auth   | 303 |
| show web-auth interface                               | 303 |
| show web-auth summary                                 | 304 |
| DHCP Snooping   | 304 |
| ip dhcp snooping                                      | 305 |
| ip dhcp snooping information option                   | 307 |
| ip dhcp snooping information option encode no-subtype | 308 |
| ip dhcp snooping information option remote-id         | 309 |
| ip dhcp snooping information policy                   | 310 |
| ip dhcp snooping verify mac-address                   | 311 |
| ip dhcp snooping vlan                                 | 311 |
| ip dhcp snooping information option circuit-id        | 312 |
| ip dhcp snooping trust                                | 313 |
| clear ip dhcp snooping binding                        | 315 |
| clear ip dhcp snooping database flash                 | 315 |
| ip dhcp snooping database flash                       | 315 |
| show ip dhcp snooping                                 | 316 |
| show ip dhcp snooping binding                         | 316 |
| IP Source Guard                                       | 316 |
| ip source-guard binding                               | 317 |
| ip source-guard                                       | 319 |
| ip source-guard max-binding                           | 320 |
| show ip source-guard                                  | 321 |
| show ip source-guard binding                          | 321 |
| ARP Inspection  | 322 |
| ip arp inspection                                     | 323 |
| ip arp inspection filter                              | 324 |
| ip arp inspection log-buffer logs                     | 325 |
| ip arp inspection validate                            | 326 |
| ip arp inspection vlan                                | 326 |
| ip arp inspection limit                               | 327 |
| ip arp inspection trust                               | 328 |

|                                       |            |
|---------------------------------------|------------|
| show ip arp inspection configuration  | 329        |
| show ip arp inspection interface      | 329        |
| show ip arp inspection log            | 330        |
| show ip arp inspection statistics     | 330        |
| show ip arp inspection vlan           | 330        |
| Denial of Service Protection          | 331        |
| dos-protection echo-charge            | 332        |
| dos-protection smurf                  | 332        |
| dos-protection tcp-flooding           | 333        |
| dos-protection tcp-null-scan          | 333        |
| dos-protection tcp-syn-fin-scan       | 334        |
| dos-protection tcp-udp-port-zero      | 334        |
| dos-protection tcp-xmas-scan          | 335        |
| dos-protection udp-flooding           | 335        |
| dos-protection win-nuke               | 336        |
| show dos-protection                   | 336        |
| Port-based Traffic Segmentation       | 337        |
| traffic-segmentation                  | 337        |
| traffic-segmentation session          | 338        |
| traffic-segmentation uplink/downlink  | 339        |
| traffic-segmentation uplink-to-uplink | 340        |
| show traffic-segmentation             | 341        |
| <b>10 Access Control Lists</b>        | <b>343</b> |
| IPv4 ACLs                             | 343        |
| access-list ip                        | 344        |
| permit, deny (Standard IP ACL)        | 345        |
| permit, deny (Extended IPv4 ACL)      | 346        |
| ip access-group                       | 348        |
| show ip access-group                  | 349        |
| show ip access-list                   | 349        |
| IPv6 ACLs                             | 350        |
| access-list ipv6                      | 350        |
| permit, deny (Standard IPv6 ACL)      | 351        |
| permit, deny (Extended IPv6 ACL)      | 353        |

|                                     |            |
|-------------------------------------|------------|
| ipv6 access-group                   | 356        |
| show ipv6 access-group              | 356        |
| show ipv6 access-list               | 357        |
| MAC ACLs                            | 358        |
| access-list mac                     | 358        |
| permit, deny (MAC ACL)              | 359        |
| mac access-group                    | 361        |
| show mac access-group               | 362        |
| show mac access-list                | 362        |
| ARP ACLs                            | 363        |
| access-list arp                     | 363        |
| permit, deny (ARP ACL)              | 364        |
| show access-list arp                | 365        |
| ACL Information                     | 365        |
| clear access-list hardware counters | 365        |
| show access-group                   | 366        |
| show access-list                    | 366        |
| <b>11 Interface Commands</b>        | <b>369</b> |
| Interface Configuration             | 370        |
| interface                           | 370        |
| alias                               | 371        |
| capabilities                        | 372        |
| description                         | 373        |
| discard                             | 374        |
| flowcontrol                         | 374        |
| history                             | 375        |
| media-type                          | 376        |
| negotiation                         | 376        |
| shutdown                            | 377        |
| speed-duplex                        | 378        |
| clear counters                      | 379        |
| show discard                        | 380        |
| show interfaces brief               | 380        |
| show interfaces counters            | 381        |

|                                       |            |
|---------------------------------------|------------|
| show interfaces history               | 385        |
| show interfaces status                | 388        |
| show interfaces switchport            | 389        |
| Transceiver Threshold Configuration   | 391        |
| transceiver-monitor                   | 391        |
| transceiver-threshold-auto            | 391        |
| transceiver-threshold current         | 392        |
| 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        |
| <b>12 Link Aggregation Commands</b>   | <b>403</b> |
| Manual Configuration Commands         | 404        |
| port channel load-balance             | 404        |
| channel-group                         | 406        |
| Dynamic Configuration Commands        | 406        |
| lacp                                  | 406        |
| lacp admin-key (Ethernet Interface)   | 408        |
| lacp port-priority                    | 409        |
| lacp system-priority                  | 410        |
| lacp admin-key (Port Channel)         | 411        |
| lacp timeout                          | 411        |
| Trunk Status Display Commands         | 412        |
| show lacp                             | 412        |
| show port-channel load-balance        | 416        |

|           |   |            |
|-----------|---|------------|
| <b>13</b> | <b>Port Mirroring Commands</b>                              | <b>417</b> |
|           | Local Port Mirroring Commands                               | 417        |
|           | port monitor  | 417        |
|           | show port monitor   | 419        |
|           | RSPAN Mirroring Commands                                    | 420        |
|           | rspan source  | 422        |
|           | rspan destination   | 423        |
|           | rspan remote vlan   | 424        |
|           | no rspan session  | 425        |
|           | show rspan  | 426        |
| <b>14</b> | <b>Congestion Control Commands</b>                          | <b>427</b> |
|           | Rate Limit Commands   | 427        |
|           | rate-limit  | 428        |
|           | Storm Control Commands                                      | 429        |
|           | switchport packet-rate                                      | 429        |
|           | Automatic Traffic Control Commands                          | 430        |
|           | Threshold Commands  | 433        |
|           | auto-traffic-control apply-timer                            | 433        |
|           | auto-traffic-control release-timer                          | 434        |
|           | auto-traffic-control  | 435        |
|           | auto-traffic-control action                                 | 435        |
|           | auto-traffic-control alarm-clear-threshold                  | 436        |
|           | auto-traffic-control alarm-fire-threshold                   | 437        |
|           | auto-traffic-control auto-control-release                   | 438        |
|           | auto-traffic-control control-release                        | 439        |
|           | SNMP Trap Commands  | 439        |
|           | snmp-server enable port-traps atc broadcast-alarm-clear     | 439        |
|           | snmp-server enable port-traps atc broadcast-alarm-fire      | 440        |
|           | snmp-server enable port-traps atc broadcast-control-apply   | 440        |
|           | snmp-server enable port-traps atc broadcast-control-release | 441        |
|           | snmp-server enable port-traps atc multicast-alarm-clear     | 441        |
|           | snmp-server enable port-traps atc multicast-alarm-fire      | 442        |
|           | snmp-server enable port-traps atc multicast-control-apply   | 442        |
|           | snmp-server enable port-traps atc multicast-control-release | 443        |

|  |            |
|--|------------|
| ATC Display Commands                             | 443        |
| show auto-traffic-control                        | 443        |
| show auto-traffic-control interface              | 444        |
| <b>15 UniDirectional Link Detection Commands</b> | <b>445</b> |
| udld detection-interval                          | 445        |
| udld message-interval                            | 446        |
| udld recovery                                    | 447        |
| udld recovery-interval                           | 447        |
| udld aggressive                                  | 448        |
| udld port  | 449        |
| show udld  | 450        |
| <b>16 Address Table Commands</b>                 | <b>453</b> |
| mac-address-table aging-time                     | 453        |
| mac-address-table static                         | 454        |
| clear mac-address-table dynamic                  | 455        |
| show mac-address-table                           | 455        |
| show mac-address-table aging-time                | 456        |
| show mac-address-table count                     | 457        |
| <b>17 Spanning Tree Commands</b>                 | <b>459</b> |
| spanning-tree                                    | 460        |
| spanning-tree cisco-prestandard                  | 461        |
| spanning-tree forward-time                       | 461        |
| spanning-tree hello-time                         | 462        |
| spanning-tree max-age                            | 463        |
| spanning-tree mode                               | 464        |
| spanning-tree pathcost method                    | 465        |
| spanning-tree priority                           | 466        |
| spanning-tree mst configuration                  | 466        |
| spanning-tree system-bpdu-flooding               | 467        |
| spanning-tree transmission-limit                 | 467        |
| max-hops   | 468        |
| mst priority                                     | 469        |
| mst vlan   | 469        |

|   |            |
|---|------------|
| name  | 470        |
| revision                                      | 471        |
| spanning-tree bpdu-filter                     | 471        |
| spanning-tree bpdu-guard                      | 472        |
| spanning-tree cost                            | 473        |
| spanning-tree edge-port                       | 474        |
| spanning-tree link-type                       | 475        |
| spanning-tree loopback-detection              | 476        |
| spanning-tree loopback-detection action       | 477        |
| spanning-tree loopback-detection release-mode | 477        |
| spanning-tree loopback-detection trap         | 478        |
| spanning-tree mst cost                        | 479        |
| spanning-tree mst port-priority               | 480        |
| spanning-tree port-bpdu-flooding              | 481        |
| spanning-tree port-priority                   | 481        |
| spanning-tree root-guard                      | 482        |
| spanning-tree spanning-disabled               | 483        |
| spanning-tree loopback-detection release      | 483        |
| spanning-tree protocol-migration              | 484        |
| show spanning-tree                            | 485        |
| show spanning-tree mst configuration          | 487        |
| <b>18 ERPS Commands</b>                       | <b>489</b> |
| erps  | 491        |
| erps domain                                   | 491        |
| control-vlan                                  | 492        |
| enable  | 493        |
| guard-timer                                   | 494        |
| holdoff-timer                                 | 494        |
| major-domain                                  | 495        |
| meg-level                                     | 496        |
| mep-monitor                                   | 497        |
| node-id                                       | 498        |
| non-erps-dev-protect                          | 499        |
| non-revertive                                 | 500        |

|                                    |            |
|------------------------------------|------------|
| propagate-tc                       | 504        |
| raps-def-mac                       | 504        |
| raps-without-vc                    | 505        |
| ring-port                          | 507        |
| rpl neighbor                       | 508        |
| rpl owner                          | 509        |
| version                            | 509        |
| wtr-timer                          | 510        |
| clear erps statistics              | 511        |
| erps clear                         | 511        |
| erps forced-switch                 | 512        |
| erps manual-switch                 | 514        |
| show erps                          | 516        |
| <b>19 VLAN Commands</b>            | <b>521</b> |
| GVRP and Bridge Extension Commands | 522        |
| bridge-ext gvrp                    | 522        |
| garp timer                         | 523        |
| switchport forbidden vlan          | 524        |
| switchport gvrp                    | 525        |
| show bridge-ext                    | 525        |
| show garp timer                    | 526        |
| show gvrp configuration            | 526        |
| Editing VLAN Groups                | 527        |
| vlan database                      | 527        |
| vlan                               | 528        |
| Configuring VLAN Interfaces        | 529        |
| interface vlan                     | 529        |
| switchport acceptable-frame-types  | 530        |
| switchport allowed vlan            | 531        |
| switchport ingress-filtering       | 532        |
| switchport mode                    | 533        |
| switchport native vlan             | 534        |
| vlan-trunking                      | 534        |

|   |     |
|---|-----|
| Displaying VLAN Information                           | 536 |
| show vlan   | 536 |
| Configuring IEEE 802.1Q Tunneling                     | 537 |
| dot1q-tunnel system-tunnel-control                    | 538 |
| switchport dot1q-tunnel mode                          | 539 |
| switchport dot1q-tunnel service match cvid            | 540 |
| switchport dot1q-tunnel tpid                          | 542 |
| show dot1q-tunnel                                     | 543 |
| Configuring L2PT Tunneling                            | 544 |
| l2protocol-tunnel tunnel-dmac                         | 544 |
| switchport l2protocol-tunnel                          | 547 |
| show l2protocol-tunnel                                | 548 |
| Configuring VLAN Translation                          | 548 |
| switchport vlan-translation                           | 548 |
| show vlan-translation                                 | 550 |
| Configuring Protocol-based VLANs                      | 550 |
| protocol-vlan protocol-group (Configuring Groups)     | 552 |
| protocol-vlan protocol-group (Configuring Interfaces) | 552 |
| show protocol-vlan protocol-group                     | 553 |
| show interfaces protocol-vlan protocol-group          | 554 |
| Configuring IP Subnet VLANs                           | 555 |
| subnet-vlan   | 555 |
| show interfaces subnet-vlan                           | 556 |
| show subnet-vlan                                      | 557 |
| Configuring MAC Based VLANs                           | 557 |
| mac-vlan  | 558 |
| show mac-vlan   | 558 |
| Configuring Voice VLANs                               | 559 |
| voice vlan  | 559 |
| voice vlan aging                                      | 560 |
| voice vlan mac-address                                | 561 |
| switchport voice vlan                                 | 562 |
| switchport voice vlan priority                        | 563 |
| switchport voice vlan rule                            | 563 |
| switchport voice vlan security                        | 564 |

|                                       |            |
|---------------------------------------|------------|
| show voice vlan                       | 565        |
| <b>20 Class of Service Commands</b>   | <b>567</b> |
| Priority Commands (Layer 2)           | 567        |
| queue mode                            | 568        |
| queue weight                          | 569        |
| switchport priority default           | 570        |
| show queue mode                       | 571        |
| show queue weight                     | 571        |
| Priority Commands (Layer 3 and 4)     | 572        |
| qos map cos-dscp                      | 572        |
| qos map dscp-cos                      | 574        |
| qos map dscp-mutation                 | 575        |
| qos map phb-queue                     | 576        |
| qos map trust-mode                    | 577        |
| show qos map cos-dscp                 | 578        |
| show qos map dscp-cos                 | 578        |
| show qos map dscp-mutation            | 579        |
| show qos map phb-queue                | 580        |
| show qos map trust-mode               | 580        |
| <b>21 Quality of Service Commands</b> | <b>583</b> |
| class-map                             | 584        |
| description                           | 585        |
| match                                 | 586        |
| rename                                | 587        |
| policy-map                            | 588        |
| bundle                                | 589        |
| class                                 | 589        |
| police flow                           | 591        |
| police srtcm-color                    | 592        |
| police trtcm-color                    | 595        |
| priority                              | 597        |
| set cos                               | 598        |
| set ip dscp                           | 598        |
| set phb                               | 599        |

|   |            |
|---|------------|
| service-policy                                  | 600        |
| show class-map                                  | 601        |
| show policy-map                                 | 601        |
| show policy-map interface                       | 602        |
| <b>22 Multicast Filtering Commands</b>          | <b>603</b> |
| IGMP Snooping                                   | 604        |
| ip igmp snooping                                | 605        |
| ip igmp snooping priority                       | 606        |
| ip igmp snooping proxy-reporting                | 607        |
| ip igmp snooping querier                        | 607        |
| ip igmp snooping router-alert-option-check      | 608        |
| ip igmp snooping router-port-expire-time        | 609        |
| ip igmp rate-limit                              | 609        |
| ip igmp snooping tcn-flood                      | 610        |
| ip igmp snooping tcn-query-solicit              | 611        |
| ip igmp snooping unregistered-data-flood        | 612        |
| ip igmp snooping unsolicited-report-interval    | 612        |
| ip igmp snooping version                        | 613        |
| ip igmp snooping version-exclusive              | 614        |
| ip igmp snooping vlan general-query-suppression | 614        |
| ip igmp snooping vlan immediate-leave           | 615        |
| ip igmp snooping vlan last-memb-query-count     | 616        |
| ip igmp snooping vlan last-memb-query-intvl     | 616        |
| ip igmp snooping vlan mrd                       | 617        |
| ip igmp snooping vlan proxy-address             | 618        |
| ip igmp snooping vlan query-interval            | 619        |
| ip igmp snooping vlan query-resp-intvl          | 620        |
| ip igmp snooping vlan static                    | 621        |
| clear ip igmp snooping groups dynamic           | 621        |
| clear ip igmp snooping statistics               | 622        |
| show ip igmp snooping                           | 622        |
| show ip igmp snooping group                     | 623        |
| show ip igmp snooping mrouter                   | 624        |
| show ip igmp snooping statistics                | 625        |

|   |     |
|---|-----|
| Static Multicast Routing                      | 628 |
| ip igmp snooping vlan mrouter                 | 628 |
| IGMP Filtering and Throttling                 | 629 |
| ip igmp filter (Global Configuration)         | 630 |
| ip igmp profile                               | 630 |
| ip igmp rate-limit                            | 631 |
| permit, deny                                  | 632 |
| range   | 632 |
| ip igmp authentication                        | 633 |
| ip igmp filter (Interface Configuration)      | 634 |
| ip igmp max-groups                            | 635 |
| ip igmp max-groups action                     | 636 |
| ip multicast-data-drop                        | 636 |
| show ip igmp authentication                   | 637 |
| show ip igmp filter                           | 638 |
| show ip igmp profile                          | 638 |
| show ip igmp rate-limit                       | 639 |
| show ip igmp throttle interface               | 640 |
| show ip multicast-data-drop                   | 640 |
| MLD Snooping                                  | 641 |
| ipv6 mld snooping                             | 642 |
| ipv6 mld snooping proxy-reporting             | 643 |
| ipv6 mld snooping querier                     | 643 |
| ipv6 mld snooping query-interval              | 644 |
| ipv6 mld snooping query-max-response-time     | 644 |
| ipv6 mld snooping robustness                  | 645 |
| ipv6 mld snooping router-port-expire-time     | 646 |
| ipv6 mld snooping unknown-multicast mode      | 646 |
| ipv6 mld snooping unsolicited-report-interval | 647 |
| ipv6 mld snooping version                     | 648 |
| ipv6 mld snooping vlan immediate-leave        | 648 |
| ipv6 mld snooping vlan mrouter                | 649 |
| ipv6 mld snooping vlan static                 | 650 |
| clear ipv6 mld snooping groups dynamic        | 650 |
| clear ipv6 mld snooping statistics            | 651 |

|   |     |
|---|-----|
| show ipv6 mld snooping                    | 651 |
| show ipv6 mld snooping group              | 652 |
| show ipv6 mld snooping group source-list  | 652 |
| show ipv6 mld snooping mrouter            | 653 |
| show ipv6 mld snooping statistics         | 654 |
| MLD Filtering and Throttling              | 655 |
| ipv6 mld filter (Global Configuration)    | 655 |
| ipv6 mld profile                          | 656 |
| permit, deny                              | 657 |
| range                                     | 657 |
| ipv6 mld filter (Interface Configuration) | 658 |
| ipv6 mld max-groups                       | 658 |
| ipv6 mld max-groups action                | 659 |
| ipv6 mld query-drop                       | 660 |
| ipv6 multicast-data-drop                  | 660 |
| show ipv6 mld filter                      | 661 |
| show ipv6 mld profile                     | 661 |
| show ipv6 mld query-drop                  | 662 |
| show ipv6 mld throttle interface          | 662 |
| MVR for IPv4                              | 664 |
| mvr                                       | 665 |
| mvr associated-profile                    | 666 |
| mvr domain                                | 666 |
| mvr priority                              | 667 |
| mvr profile                               | 667 |
| mvr proxy-query-interval                  | 668 |
| mvr proxy-switching                       | 669 |
| mvr robustness-value                      | 670 |
| mvr source-port-mode dynamic              | 671 |
| mvr upstream-source-ip                    | 671 |
| mvr vlan                                  | 672 |
| mvr immediate-leave                       | 673 |
| mvr type                                  | 674 |
| mvr vlan group                            | 675 |
| clear mrv groups dynamic                  | 676 |

|                               |            |
|-------------------------------|------------|
| clear mrv statistics          | 676        |
| show mvr                      | 677        |
| show mvr associated-profile   | 678        |
| show mvr interface            | 678        |
| show mvr members              | 680        |
| show mvr profile              | 681        |
| show mvr statistics           | 682        |
| MVR for IPv6                  | 687        |
| mvr6 associated-profile       | 688        |
| mvr6 domain                   | 689        |
| mvr6 priority                 | 690        |
| mvr6 profile                  | 690        |
| mvr6 proxy-query-interval     | 691        |
| mvr6 proxy-switching          | 692        |
| mvr6 robustness-value         | 693        |
| mvr6 source-port-mode dynamic | 694        |
| mvr6 upstream-source-ip       | 694        |
| mvr6 vlan                     | 695        |
| mvr6 immediate-leave          | 696        |
| mvr6 type                     | 697        |
| mvr6 vlan group               | 698        |
| clear mvr6 groups dynamic     | 699        |
| clear mvr6 statistics         | 699        |
| show mvr6                     | 700        |
| show mvr6 associated-profile  | 701        |
| show mvr6 interface           | 702        |
| show mvr6 members             | 703        |
| show mvr6 profile             | 704        |
| show mvr6 statistics          | 704        |
| <b>23 LLDP Commands</b>       | <b>711</b> |
| lldp                          | 713        |
| lldp holdtime-multiplier      | 713        |
| lldp med-fast-start-count     | 714        |
| lldp notification-interval    | 714        |

|                                      |            |
|--------------------------------------|------------|
| lldp refresh-interval                | 715        |
| lldp reinit-delay                    | 715        |
| lldp tx-delay                        | 716        |
| lldp admin-status                    | 717        |
| lldp basic-tlv management-ip-address | 717        |
| lldp basic-tlv port-description      | 718        |
| lldp basic-tlv system-capabilities   | 718        |
| lldp basic-tlv system-description    | 719        |
| lldp basic-tlv system-name           | 719        |
| lldp dot1-tlv proto-ident            | 720        |
| lldp dot1-tlv proto-vid              | 720        |
| lldp dot1-tlv pvid                   | 721        |
| lldp dot1-tlv vlan-name              | 721        |
| lldp dot3-tlv link-agg               | 722        |
| lldp dot3-tlv mac-phy                | 722        |
| lldp dot3-tlv max-frame              | 723        |
| lldp med-location civic-addr         | 724        |
| lldp med-notification                | 725        |
| lldp med-tlv inventory               | 726        |
| lldp med-tlv location                | 727        |
| lldp med-tlv med-cap                 | 727        |
| lldp med-tlv network-policy          | 728        |
| lldp notification                    | 728        |
| show lldp config                     | 729        |
| show lldp info local-device          | 730        |
| show lldp info remote-device         | 731        |
| show lldp info statistics            | 733        |
| <b>24 CFM Commands</b>               | <b>735</b> |
| Defining CFM Structures              | 738        |
| ethernet cfm ais level               | 738        |
| ethernet cfm ais ma                  | 739        |
| ethernet cfm ais period              | 740        |
| ethernet cfm ais suppress alarm      | 740        |
| ethernet cfm domain                  | 741        |

|  |     |
|--|-----|
| ethernet cfm enable                                    | 743 |
| ma index name  | 744 |
| ma index name-format                                   | 745 |
| ethernet cfm mep                                       | 746 |
| ethernet cfm port-enable                               | 747 |
| clear ethernet cfm ais mpid                            | 747 |
| show ethernet cfm configuration                        | 748 |
| show ethernet cfm md                                   | 749 |
| show ethernet cfm ma                                   | 750 |
| show ethernet cfm maintenance-points local             | 751 |
| show ethernet cfm maintenance-points local detail mep  | 752 |
| show ethernet cfm maintenance-points remote detail     | 753 |
| Continuity Check Operations                            | 755 |
| ethernet cfm cc ma interval                            | 755 |
| ethernet cfm cc enable                                 | 756 |
| snmp-server enable traps ethernet cfm cc               | 757 |
| mep archive-hold-time                                  | 758 |
| clear ethernet cfm maintenance-points remote           | 758 |
| clear ethernet cfm errors                              | 759 |
| show ethernet cfm errors                               | 760 |
| Cross Check Operations                                 | 761 |
| ethernet cfm mep crosscheck start-delay                | 761 |
| snmp-server enable traps ethernet cfm crosscheck       | 761 |
| mep crosscheck mpid                                    | 762 |
| ethernet cfm mep crosscheck                            | 763 |
| show ethernet cfm maintenance-points remote crosscheck | 764 |
| Link Trace Operations                                  | 764 |
| ethernet cfm linktrace cache                           | 764 |
| ethernet cfm linktrace cache hold-time                 | 765 |
| ethernet cfm linktrace cache size                      | 766 |
| ethernet cfm linktrace                                 | 767 |
| clear ethernet cfm linktrace-cache                     | 768 |
| show ethernet cfm linktrace-cache                      | 768 |
| Loopback Operations                                    | 770 |
| ethernet cfm loopback                                  | 770 |

|  |            |
|--|------------|
| Fault Generator Operations               | 771        |
| mep fault-notify alarm-time              | 771        |
| mep fault-notify lowest-priority         | 772        |
| mep fault-notify reset-time              | 773        |
| show ethernet cfm fault-notify-generator | 774        |
| Delay Measure Operations                 | 775        |
| ethernet cfm delay-measure two-way       | 775        |
| <b>25 OAM Commands</b>                   | <b>777</b> |
| efm oam                                  | 778        |
| efm oam critical-link-event              | 778        |
| efm oam link-monitor frame               | 779        |
| efm oam link-monitor frame threshold     | 780        |
| efm oam link-monitor frame window        | 780        |
| efm oam mode                             | <b>781</b> |
| clear efm oam counters                   | 782        |
| clear efm oam event-log                  | 782        |
| efm oam remote-loopback                  | 783        |
| efm oam remote-loopback test             | 784        |
| show efm oam counters interface          | 785        |
| show efm oam event-log interface         | 785        |
| show efm oam remote-loopback interface   | 787        |
| show efm oam status interface            | 787        |
| show efm oam status remote interface     | 788        |
| <b>26 Domain Name Service Commands</b>   | <b>789</b> |
| ip domain-list                           | 789        |
| ip domain-lookup                         | 790        |
| ip domain-name                           | 791        |
| ip host                                  | 792        |
| ip name-server                           | 793        |
| ipv6 host                                | 794        |
| clear dns cache                          | 794        |
| clear host                               | 795        |
| show dns                                 | 795        |
| show dns cache                           | 796        |

|                                    |            |
|------------------------------------|------------|
| show hosts                         | 796        |
| <b>27 DHCP Commands</b>            | <b>799</b> |
| DHCP Client                        | 799        |
| DHCP for IPv4                      | 800        |
| ip dhcp dynamic-provision          | 800        |
| ip dhcp client class-id            | 801        |
| ip dhcp restart client             | 803        |
| show ip dhcp dynamic-provision     | 803        |
| DHCP for IPv6                      | 804        |
| ipv6 dhcp client rapid-commit vlan | 804        |
| ipv6 dhcp restart client vlan      | 804        |
| show ipv6 dhcp duid                | 806        |
| show ipv6 dhcp vlan                | 806        |
| DHCP Relay Option 82               | 807        |
| ip dhcp relay server               | 807        |
| ip dhcp relay information option   | 808        |
| ip dhcp relay information policy   | 811        |
| show ip dhcp relay                 | 812        |
| <b>28 IP Interface Commands</b>    | <b>813</b> |
| IPv4 Interface                     | 813        |
| Basic IPv4 Configuration           | 814        |
| ip address                         | 814        |
| ip default-gateway                 | 816        |
| show ip default-gateway            | 816        |
| show ip interface                  | 817        |
| show ip traffic                    | 817        |
| traceroute                         | 818        |
| ping                               | 820        |
| ARP Configuration                  | 821        |
| arp timeout                        | 821        |
| clear arp-cache                    | 822        |
| show arp                           | 822        |

|  |     |
|--|-----|
| IPv6 Interface                                   | 823 |
| Interface Address Configuration and Utilities    | 824 |
| ipv6 default-gateway                             | 824 |
| ipv6 address                                     | 825 |
| ipv6 address autoconfig                          | 826 |
| ipv6 address eui-64                              | 828 |
| ipv6 address link-local                          | 829 |
| ipv6 enable                                      | 831 |
| ipv6 mtu   | 832 |
| show ipv6 default-gateway                        | 833 |
| show ipv6 interface                              | 833 |
| show ipv6 mtu                                    | 835 |
| show ipv6 traffic                                | 836 |
| clear ipv6 traffic                               | 840 |
| ping6  | 840 |
| traceroute6                                      | 842 |
| Neighbor Discovery                               | 843 |
| ipv6 hop-limit                                   | 843 |
| ipv6 nd dad attempts                             | 844 |
| ipv6 nd ns-interval                              | 845 |
| ipv6 nd rguard                                   | 846 |
| ipv6 nd reachable-time                           | 847 |
| clear ipv6 neighbors                             | 848 |
| show ipv6 nd rguard                              | 848 |
| show ipv6 neighbors                              | 849 |
| ND Snooping                                      | 850 |
| ipv6 nd snooping                                 | 851 |
| ipv6 nd snooping auto-detect                     | 853 |
| ipv6 nd snooping auto-detect retransmit count    | 853 |
| ipv6 nd snooping auto-detect retransmit interval | 854 |
| ipv6 nd snooping prefix timeout                  | 854 |
| ipv6 nd snooping max-binding                     | 855 |
| ipv6 nd snooping trust                           | 855 |
| clear ipv6 nd snooping binding                   | 856 |
| clear ipv6 nd snooping prefix                    | 856 |

|                               |     |
|-------------------------------|-----|
| show ipv6 nd snooping         | 857 |
| show ipv6 nd snooping binding | 857 |
| show ipv6 nd snooping prefix  | 858 |

---

|                    |   |            |
|--------------------|---|------------|
| <b>Section III</b> | <b>Appendices</b>                           | <b>859</b> |
|                    | <b>A Troubleshooting</b>                    | <b>861</b> |
|                    | Problems Accessing the Management Interface | 861        |
|                    | Using System Logs                           | 862        |
|                    | <b>B License Information</b>                | <b>863</b> |
|                    | The GNU General Public License              | 863        |
|                    | <b>Glossary</b>                             | <b>867</b> |
|                    | <b>Command List</b>                         | <b>875</b> |
|                    | <b>Index</b>                                | <b>883</b> |

---

# Figures

|  |     |
|--|-----|
| Figure 1: Storm Control by Limiting the Traffic Rate | 432 |
| Figure 2: Storm Control by Shutting Down a Port      | 433 |
| Figure 3: Non-ERPS Device Protection                 | 499 |
| Figure 4: Sub-ring with Virtual Channel              | 506 |
| Figure 5: Sub-ring without Virtual Channel           | 507 |
| Figure 6: Configuring VLAN Trunking                  | 535 |
| Figure 7: Mapping QinQ Service VLAN to Customer VLAN | 541 |
| Figure 8: Configuring VLAN Translation               | 549 |



---

# Tables

|  |     |
|--|-----|
| Table 1: Options 60, 66 and 67 Statements              | 60  |
| Table 2: Options 55 and 124 Statements                 | 60  |
| Table 3: General Command Modes                         | 75  |
| Table 4: Configuration Command Modes                   | 77  |
| Table 5: Keystroke Commands                            | 78  |
| Table 6: Command Group Index                           | 79  |
| Table 7: General Commands                              | 83  |
| Table 8: System Management Commands                    | 91  |
| Table 9: Device Designation Commands                   | 91  |
| Table 10: Banner Commands                              | 92  |
| Table 11: System Status Commands                       | 101 |
| Table 12: show process cpu guard - display description | 105 |
| Table 13: Frame Size Commands                          | 112 |
| Table 14: Flash/File Commands                          | 113 |
| Table 15: File Directory Information                   | 119 |
| Table 16: Line Commands                                | 125 |
| Table 17: Event Logging Commands                       | 136 |
| Table 18: Logging Levels                               | 137 |
| Table 19: show logging flash/ram - display description | 142 |
| Table 20: show logging trap - display description      | 142 |
| Table 21: Event Logging Commands                       | 142 |
| Table 22: Time Commands                                | 146 |
| Table 23: Predefined Summer-Time Parameters            | 151 |
| Table 24: Time Range Commands                          | 155 |
| Table 25: Sync-E Commands                              | 159 |
| Table 26: Synchronous Ethernet Standards               | 160 |
| Table 27: show sync - display description for sync     | 167 |
| Table 28: Switch Cluster Commands                      | 168 |
| Table 29: SNMP Commands                                | 175 |

|  |     |
|--|-----|
| Table 30: show snmp engine-id - display description                      | 190 |
| Table 31: show snmp group - display description                          | 191 |
| Table 32: show snmp user - display description                           | 192 |
| Table 33: show snmp view - display description                           | 193 |
| Table 34: RMON Commands  | 201 |
| Table 35: sFlow Commands   | 209 |
| Table 36: Authentication Commands  | 215 |
| Table 37: User Access Commands   | 216 |
| Table 38: Default Login Settings   | 217 |
| Table 39: Authentication Sequence Commands                               | 218 |
| Table 40: RADIUS Client Commands   | 220 |
| Table 41: TACACS+ Client Commands  | 224 |
| Table 42: AAA Commands   | 228 |
| Table 43: Web Server Commands  | 236 |
| Table 44: HTTPS System Support   | 239 |
| Table 45: Telnet Server Commands   | 239 |
| Table 46: Secure Shell Commands  | 242 |
| Table 47: show ssh - display description                                 | 251 |
| Table 48: 802.1X Port Authentication Commands                            | 252 |
| Table 49: Management IP Filter Commands                                  | 268 |
| Table 50: PPPoE Intermediate Agent Commands                              | 270 |
| Table 51: show pppoe intermediate-agent statistics - display description | 276 |
| Table 52: General Security Commands                                      | 279 |
| Table 53: Management IP Filter Commands                                  | 280 |
| Table 54: show port security - display description                       | 283 |
| Table 55: Network Access Commands  | 284 |
| Table 56: Dynamic QoS Profiles   | 288 |
| Table 57: Web Authentication   | 298 |
| Table 58: DHCP Snooping Commands   | 304 |
| Table 59: Option 82 information  | 313 |
| Table 60: IP Source Guard Commands                                       | 316 |
| Table 61: ARP Inspection Commands  | 322 |
| Table 62: DoS Protection Commands  | 331 |
| Table 63: Commands for Configuring Traffic Segmentation                  | 337 |
| Table 64: Traffic Segmentation Forwarding                                | 338 |

|   |     |
|---|-----|
| Table 65: Access Control List Commands                        | 343 |
| Table 66: IPv4 ACL Commands                                   | 343 |
| Table 67: IPv6 ACL Commands                                   | 350 |
| Table 68: MAC ACL Commands                                    | 358 |
| Table 69: ARP ACL Commands                                    | 363 |
| Table 70: ACL Information Commands                            | 365 |
| Table 71: Interface Commands                                  | 369 |
| Table 72: show interfaces counters - display description      | 382 |
| Table 73: show interfaces switchport - display description    | 390 |
| Table 74: Link Aggregation Commands                           | 403 |
| Table 75: show lacp counters - display description            | 413 |
| Table 76: show lacp internal - display description            | 413 |
| Table 77: show lacp neighbors - display description           | 415 |
| Table 78: show lacp sysid - display description               | 415 |
| Table 79: Port Mirroring Commands                             | 417 |
| Table 80: Mirror Port Commands                                | 417 |
| Table 81: RSPAN Commands                                      | 420 |
| Table 82: Congestion Control Commands                         | 427 |
| Table 83: Rate Limit Commands                                 | 427 |
| Table 84: Rate Limit Commands                                 | 429 |
| Table 85: ATC Commands  | 430 |
| Table 86: UniDirectional Link Detection Commands              | 445 |
| Table 87: show udld - display description                     | 450 |
| Table 88: Address Table Commands                              | 453 |
| Table 89: Spanning Tree Commands                              | 459 |
| Table 90: Recommended STA Path Cost Range                     | 473 |
| Table 91: Default STA Path Costs                              | 474 |
| Table 92: ERPS Commands                                       | 489 |
| Table 93: ERPS Request/State Priority                         | 513 |
| Table 94: show erps - summary display description             | 516 |
| Table 95: show erps domain - detailed display description     | 518 |
| Table 96: show erps statistics - detailed display description | 519 |
| Table 97: VLAN Commands                                       | 521 |
| Table 98: GVRP and Bridge Extension Commands                  | 522 |
| Table 99: Commands for Editing VLAN Groups                    | 527 |

|  |     |
|--|-----|
| Table 100: Commands for Configuring VLAN Interfaces                          | 529 |
| Table 101: Commands for Displaying VLAN Information                          | 536 |
| Table 102: 802.1Q Tunneling Commands   | 537 |
| Table 103: L2 Protocol Tunnel Commands                                       | 544 |
| Table 104: VLAN Translation Commands   | 548 |
| Table 105: Protocol-based VLAN Commands                                      | 551 |
| Table 106: IP Subnet VLAN Commands   | 555 |
| Table 107: MAC Based VLAN Commands   | 557 |
| Table 108: Voice VLAN Commands   | 559 |
| Table 109: Priority Commands   | 567 |
| Table 110: Priority Commands (Layer 2)                                       | 567 |
| Table 111: Priority Commands (Layer 3 and 4)                                 | 572 |
| Table 112: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence        | 573 |
| Table 113: Mapping Internal PHB/Drop Precedence to CoS/CFI Values            | 574 |
| Table 114: Default Mapping of DSCP Values to Internal PHB/Drop Values        | 575 |
| Table 115: Mapping Internal Per-hop Behavior to Hardware Queues              | 576 |
| Table 116: Quality of Service Commands                                       | 583 |
| Table 117: Multicast Filtering Commands                                      | 603 |
| Table 118: IGMP Snooping Commands  | 604 |
| Table 119: show ip igmp snooping statistics input - display description      | 626 |
| Table 120: show ip igmp snooping statistics output - display description     | 626 |
| Table 121: show ip igmp snooping statistics vlan query - display description | 627 |
| Table 122: Static Multicast Interface Commands                               | 628 |
| Table 123: IGMP Filtering and Throttling Commands                            | 629 |
| Table 124: IGMP Authentication RADIUS Attribute Value Pairs                  | 634 |
| Table 125: MLD Snooping Commands   | 641 |
| Table 126: MLD Filtering and Throttling Commands                             | 655 |
| Table 127: Multicast VLAN Registration for IPv4 Commands                     | 664 |
| Table 128: show mvr - display description                                    | 677 |
| Table 129: show mvr interface - display description                          | 679 |
| Table 130: show mvr members - display description                            | 681 |
| Table 131: show mvr statistics input - display description                   | 682 |
| Table 132: show mvr statistics output - display description                  | 683 |
| Table 133: show mvr statistics query - display description                   | 684 |
| Table 134: show mvr statistics summary interface - display description       | 685 |

|  |     |
|--|-----|
| Table 135: show mvr statistics summary interface mvr vlan - description    | 686 |
| Table 136: Multicast VLAN Registration for IPv6 Commands                   | 687 |
| Table 137: show mvr6 - display description                                 | 700 |
| Table 138: show mvr6 interface - display description                       | 702 |
| Table 139: show mvr6 members - display description                         | 704 |
| Table 140: show mvr6 statistics input - display description                | 705 |
| Table 141: show mvr6 statistics output - display description               | 706 |
| Table 142: show mvr6 statistics query - display description                | 706 |
| Table 143: show mvr6 statistics summary interface - display description    | 707 |
| Table 144: show mvr6 statistics summary interface mvr vlan - description   | 708 |
| Table 145: LLDP Commands   | 711 |
| Table 146: LLDP MED Location CA Types                                      | 724 |
| Table 147: CFM Commands  | 735 |
| Table 148: show ethernet cfm configuration traps - display description     | 749 |
| Table 149: show ethernet cfm maintenance-points local detail mep - display | 753 |
| Table 150: show ethernet cfm maintenance-points remote detail - display    | 754 |
| Table 151: show ethernet cfm errors - display description                  | 760 |
| Table 152: show ethernet cfm linktrace-cache - display description         | 768 |
| Table 153: Remote MEP Priority Levels                                      | 772 |
| Table 154: MEP Defect Descriptions   | 773 |
| Table 155: show fault-notify-generator - display description               | 774 |
| Table 156: OAM Commands  | 777 |
| Table 157: Address Table Commands  | 789 |
| Table 158: show dns cache - display description                            | 796 |
| Table 159: show hosts - display description                                | 797 |
| Table 160: DHCP Commands   | 799 |
| Table 161: DHCP Client Commands  | 799 |
| Table 162: Options 60, 66 and 67 Statements                                | 802 |
| Table 163: Options 55 and 124 Statements                                   | 802 |
| Table 164: DHCP Relay Option 82 Commands                                   | 807 |
| Table 165: IP Interface Commands   | 813 |
| Table 166: IPv4 Interface Commands   | 813 |
| Table 167: Basic IP Configuration Commands                                 | 814 |
| Table 168: Address Resolution Protocol Commands                            | 821 |
| Table 169: IPv6 Configuration Commands                                     | 823 |

---

## Tables

|  |     |
|--|-----|
| Table 170: show ipv6 interface - display description | 834 |
| Table 171: show ipv6 mtu - display description       | 835 |
| Table 172: show ipv6 traffic - display description   | 837 |
| Table 173: show ipv6 neighbors - display description | 849 |
| Table 174: ND Snooping Commands                      | 851 |
| Table 175: Troubleshooting Chart                     | 861 |

# Section I

## Getting Started

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- ◆ ["Initial Switch Configuration" on page 49](#)



# 1

## 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 53](#).

---

### 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 a management 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

- ◆ Filter packets using Access Control Lists (ACLs)
- ◆ Configure up to 4093 IEEE 802.1Q VLANs
- ◆ Enable GVRP automatic VLAN registration
- ◆ Configure IP routing for unicast traffic
- ◆ Configure router redundancy
- ◆ Configure IGMP multicast filtering
- ◆ Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/TFTP (using the command line or web interface)
- ◆ Configure Spanning Tree parameters
- ◆ Configure Class of Service (CoS) priority queuing
- ◆ Configure static or LACP trunks (up to 12)
- ◆ Enable port mirroring
- ◆ Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- ◆ Display system information and statistics

**Required Connections** 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-232 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.



**Note:** Once you have set up the terminal correctly, the console login screen will be displayed.

---

For a description of how to use the CLI, see [“Using the Command Line Interface” on page 69](#). For a list of all the CLI commands and detailed information on using the CLI, refer to [“CLI Command Groups” on page 79](#).

## Remote Connections

Prior to accessing the switch’s onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, or DHCP protocol.

An IPv4 address for this 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 53](#).



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

---

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 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.

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.



**Note:** The switch also includes a Craft port on the front panel which provides a secure management connection that is isolated from all other ports on the switch. This interface is not configured with an IP address by default, but may be manually configured with an IPv4 or IPv6 address as described in the following sections. The Craft port can only be configured through the command line interface, and is specified with the name “craft” in the commands used to configure its IP address.

---

## Basic Configuration

**Console Connection** 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, also enter “admin.” (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 and password “admin” 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>.
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 ECS4810-12M 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)#
```

**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 can 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 58](#).

DHCP for IPv6 can be used to acquire stateful address configuration information depending on the advertisements received from other routers, and subsequently from a DHCPv6 server. (For more information, see the description for the “Restart DHCPv6” parameter under “Configuring IPv6 Interface Settings” in the *Web Management Guide*.)

### 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 IP 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, under “Configuring IPv6 Interface Settings” in the *Web Management Guide*.

**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>.

```

Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
(None)
Joined group address(es):
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#

```

**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::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
    2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
ff02::1:ff00:0
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>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 70-72-CF-1C-BA-52
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

### 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>.

```
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::7272:cfff:fe1c:ba52%1/64
Global unicast address(es):
  (None)
Joined group address(es):
  ff02::1:ff1c:ba52
  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#
```

**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 will also be supported in future software releases.)

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 address autoconfig
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
 fe80::260:3fff:fe11:6700/64
Global unicast address(es):
 2001:db8:2222:7272:2e0:cff:fe00:fd/64, subnet is 2001:db8:2222:7272::/
 64[AUTOCONFIG]
   valid lifetime 2591978 preferred lifetime 604778
Joined group address(es):
 ff02::1:ff00:0
 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#
```

### Downloading a Configuration File Referenced 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**

| Option | Statement               |   |
|--------|-------------------------|---|
|        | Keyword                 | Parameter                                       |
| 60     | vendor-class-identifier | a string indicating the vendor class identifier |
| 66     | tftp-server-name        | a string indicating the tftp server name        |
| 67     | bootfile-name           | a string indicating the bootfile name           |

- ◆ 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" 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**

| Option | Statement                   |   |
|--------|-----------------------------|---|
|        | Keyword                     | Parameter                                       |
| 55     | dhcp-parameter-request-list | a list of parameters, separated by "            |
| 124    | vendor-class-identifier     | a string indicating the vendor class identifier |

The following configuration examples are 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 = "ecs-runtime.bix";
    option tftp-server-name "192.168.255.101";
    option bootfile-name "test";
}
```



**Note:** Use “ecs-runtime.bix” for the vendor-class-identifier in the dhcpd.conf file.

### Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as Edge-Core ECView Pro. 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 (under "Setting SNMPv3 Views" in the *Web Management Guide*).

### 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 “snmp-server host” on page 182. 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 mib-2 802.1d
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 *Web Management Guide*, or refer to the specific CLI commands for SNMP starting on page 175.

---

## Managing System Files

The switch’s flash memory supports three types of system files that can be managed by the CLI program, 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 64](#) 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. See "Managing System Files" in the *Web Management Guide* for more information.
- ◆ **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

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.

### **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#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#
```



# Section II

## 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:

- ◆ ["Using the Command Line Interface" on page 69](#)
- ◆ ["General Commands" on page 83](#)
- ◆ ["System Management Commands" on page 91](#)
- ◆ ["SNMP Commands" on page 175](#)
- ◆ ["Remote Monitoring Commands" on page 201](#)
- ◆ ["Authentication Commands" on page 215](#)
- ◆ ["General Security Measures" on page 279](#)
- ◆ ["Access Control Lists" on page 343](#)
- ◆ ["Interface Commands" on page 369](#)
- ◆ ["Link Aggregation Commands" on page 403](#)
- ◆ ["Port Mirroring Commands" on page 417](#)
- ◆ ["Congestion Control Commands" on page 427](#)
- ◆ ["UniDirectional Link Detection Commands" on page 445](#)
- ◆ ["Address Table Commands" on page 453](#)
- ◆ ["Spanning Tree Commands" on page 459](#)
- ◆ ["ERPS Commands" on page 489](#)

- ◆ "VLAN Commands" on page 521
- ◆ "Class of Service Commands" on page 567
- ◆ "Quality of Service Commands" on page 583
- ◆ "Multicast Filtering Commands" on page 603
- ◆ "LLDP Commands" on page 711
- ◆ "CFM Commands" on page 735
- ◆ "OAM Commands" on page 777
- ◆ "Domain Name Service Commands" on page 789
- ◆ "DHCP Commands" on page 799
- ◆ "IP Interface Commands" on page 813

# 2

## 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 ECS4810-12M 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 10.1.0.254 255.255.255.0
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 ECS4810-12M is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```



**Note:** You can open up to eight sessions to the device via Telnet.

---

## 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:

```
Console>enable  
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 “**system ?**” displays a list of possible system commands:

```
Console#show ?
  access-group      Access groups
  access-list       Access lists
  accounting         Uses an accounting list with this name
  alarm             Alarm
  alarm-status      Show alarm status
  arp               Information of ARP cache
  authorization      Enables EXEC accounting
  auto-traffic-control Auto traffic control information
  banner            Banner info
  bridge-ext        Bridge extension information
  cable-diagnostics Shows the information of cable diagnostics
  calendar          Date and time information
  class-map         Displays class maps
  cluster           Display cluster
  debug             State of each debugging option
  discard           Discard packet
  dns               DNS information
  dos-protection    Shows the system dos-protection summary information
  dot1q-tunnel      dot1q-tunnel
  dot1x             802.1X content
  efm               Ethernet First Mile feature
  erps              Displays ERPS configuration
  ethernet          Specifies the ethernet
  garp              GARP properties
  gvrp              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
  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
  network-access    Shows the entries of the secure port.
  nlm               Show notification log
  policy-map        Displays policy maps
  port              Port characteristics
  port-channel      Port channel information
```

|                      |   |
|----------------------|---|
| power-save           | Shows the power saving information                              |
| pppoe                | Displays PPPoE configuration                                    |
| process              | Device process  |
| protocol-vlan        | Protocol-VLAN information                                       |
| public-key           | Public key information  |
| qos                  | Quality of Service  |
| queue                | Priority queue information                                      |
| radius-server        | RADIUS server information                                       |
| reload               | Shows the reload settings                                       |
| rmon                 | Remote Monitoring Protocol                                      |
| rspan                | Display status of the current RSPAN configuration               |
| running-config       | Information on the running configuration                        |
| sflow                | Shows the sflow information                                     |
| snmp                 | Simple Network Management Protocol configuration and statistics |
| snmp-server          | Displays SNMP server configuration                              |
| sntp                 | Simple Network Time Protocol configuration                      |
| spanning-tree        | Spanning-tree configuration                                     |
| ssh                  | Secure shell server connections                                 |
| startup-config       | Startup system configuration                                    |
| subnet-vlan          | IP subnet-based VLAN information                                |
| sync                 | Shows synchronous ethernet status                               |
| system               | System information  |
| tacacs-server        | TACACS server information                                       |
| tech-support         | Technical information   |
| time-range           | Time range  |
| traffic-segmentation | Traffic segmentation information                                |
| udld                 | Displays UDLD information                                       |
| upgrade              | Shows upgrade information                                       |
| users                | Information about users logged in                               |
| version              | System hardware and software versions                           |
| vlan                 | Shows virtual LAN settings                                      |
| vlan-translation     | VLAN translation information                                    |
| voice                | Shows the voice VLAN information                                |
| watchdog             | Displays watchdog status  |
| web-auth             | Shows web authentication configuration                          |

Console#show

The command “**show interfaces ?**” will display the following information:

```
Console#show interfaces ?
brief           Shows brief interface description
counters        Interface counters information
craft           Shows craft port link information
history         Historical sample of interface counters information
protocol-vlan   Protocol-VLAN information
status          Shows interface status
subnet-vlan     IP subnet-based VLAN information
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?  
sflow          snmp          snmp-server   snmp          spanning-tree  
ssh            startup-config subnet-vlan    synce         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 3: General Command Modes**

| Class         | Mode   |
|---------------|--|
| Exec          | Normal<br>Privileged   |
| Configuration | Global*<br>Access Control List<br>CFM<br>Class Map<br>ERPS<br>IGMP Profile<br>Interface<br>Line<br>Multiple Spanning Tree<br>Policy Map<br>Time Range<br>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 and password “admin.” 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 ECS4810-12M is opened.
To end the CLI session, enter [Exit].

Console#
    
```

```

Username: guest
Password: [guest login password]

CLI session with the ECS4810-12M 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.
- ◆ CFM Configuration - Configures connectivity monitoring using continuity check messages, fault verification through loopback messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices.
- ◆ Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- ◆ ERPS Configuration – These commands configure Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks.
- ◆ 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**

| Mode                | Command  | Prompt                       | Page                |
|---------------------|--|------------------------------|---------------------|
| Access Control List | access-list arp  | Console(config-arp-acl)      | <a href="#">363</a> |
|                     | access-list ip standard  | Console(config-std-acl)      | <a href="#">344</a> |
|                     | access-list ip extended  | Console(config-ext-acl)      | <a href="#">344</a> |
|                     | access-list ipv6 standard  | Console(config-std-ipv6-acl) | <a href="#">350</a> |
|                     | access-list ipv6 extended  | Console(config-ext-ipv6-acl) | <a href="#">350</a> |
|                     | access-list mac  | Console(config-mac-acl)      | <a href="#">358</a> |
| CFM                 | ethernet cfm domain  | Console(config-ether-cfm)    | <a href="#">741</a> |
| Class Map           | class-map  | Console(config-cmap)         | <a href="#">584</a> |
| ERPS                | erps domain  | Console(config-erps)         | <a href="#">491</a> |
| Interface           | interface {ethernet <i>port</i>   port-channel <i>id</i>  <br>vlan <i>id</i> } | Console(config-if)           | <a href="#">370</a> |
| Line                | line {console   vty}   | Console(config-line)         | <a href="#">125</a> |
| MSTP                | spanning-tree mst-configuration  | Console(config-mstp)         | <a href="#">466</a> |
| Policy Map          | policy-map   | Console(config-pmap)         | <a href="#">588</a> |
| Time Range          | time-range   | Console(config-time-range)   | <a href="#">155</a> |
| VLAN                | vlan database  | Console(config-vlan)         | <a href="#">527</a> |

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**

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

**Showing Status Information** There are various “show” commands which display configuration settings or the status of specified processes. Many of these commands will not display any information unless the switch is properly configured, and in some cases the interface to which a command applies is up.

For example, if a static router port is configured, the corresponding show command will not display any information unless IGMP snooping is enabled, and the link for the static router port is up.

```
Console#configure
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#end
Console#show ip igmp snooping mrouter
  VLAN M'cast Router Ports Type
  ----
Console#configure
Console(config)#ip igmp snooping
```

```

Console(config)#end
Console#show ip igmp snooping mrouter
  VLAN M'cast Router Ports Type
  ----
  1    Eth 1/11                Static
Console#
    
```

**Output Modifiers** Some of the show commands include options for output modifiers. For example, the “show running-config” command includes the following keyword options:

```

Console#show running-config ?
| Output modifiers
<cr>
    
```

The output modifiers include options which indicate a string that occurs at the beginning of a line, in lines that are to be excluded, or in lines that are to be included.

```

Console#show running-config | ?
begin      Begin with line that matches
exclude    Exclude lines that match
include    Include lines that match
    
```

Note that the output modifier `begin` can only be used as the first modifier if more than one modifier is used in a command.

## CLI Command Groups

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

**Table 6: Command Group Index**

| Command Group                      | Description   | Page                |
|------------------------------------|---|---------------------|
| General                            | Basic commands for entering privileged access mode, restarting the system, or quitting the CLI  | <a href="#">83</a>  |
| System Management                  | 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 | <a href="#">91</a>  |
| Simple Network Management Protocol | Activates authentication failure traps; configures community access strings, and trap receivers   | <a href="#">175</a> |
| Remote Monitoring                  | Supports statistics, history, alarm and event groups  | <a href="#">201</a> |
| Flow Sampling                      | Samples traffic flows, and forwards data to designated collector  | <a href="#">209</a> |

**Table 6: Command Group Index** (Continued)

| <b>Command Group</b>          | <b>Description</b>   | <b>Page</b> |
|-------------------------------|--|-------------|
| User Authentication           | 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 | 215         |
| General Security Measures     | 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         | 279         |
| Access Control List           | Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header), or non-IP frames (based on MAC address or Ethernet type)   | 343         |
| Interface                     | Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs   | 369         |
| Link Aggregation              | Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks   | 403         |
| Mirror Port                   | Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port  | 417         |
| Congestion Control            | 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.   | 427         |
| Loopback Detection            | Detects general loopback conditions caused by hardware problems or faulty protocol settings  | 385         |
| UniDirectional Link Detection | Detect and disables unidirectional links   | 445         |
| Address Table                 | Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time   | 453         |
| Spanning Tree                 | Configures Spanning Tree settings for the switch   | 459         |
| ERPS                          | Configures Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks  | 489         |
| VLANs                         | Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling   | 521         |
| Class of Service              | Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for DSCP  | 567         |
| Quality of Service            | Configures Differentiated Services   | 583         |
| Multicast Filtering           | Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration   | 603         |
| Link Layer Discovery Protocol | Configures LLDP settings to enable information discovery about neighbor devices  | 711         |

**Table 6: Command Group Index** (Continued)

| Command Group                       | Description  | Page |
|-------------------------------------|--|------|
| Connectivity Fault Management       | Configures connectivity monitoring using continuity check messages, fault verification through loopback messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices | 735  |
| OAM                                 | Configures Operations, Administration and Maintenance remote management tools required to monitor and maintain the links to subscriber CPEs  | 777  |
| Domain Name Service                 | Configures DNS services.   | 789  |
| Dynamic Host Configuration Protocol | Configures DHCP client functions   | 799  |
| IP Interface                        | Configures IP address for the switch interfaces; also configures ARP parameters  | 813  |
| Debug                               | Displays debugging information for all key functions<br>These commands are not described in this manual.<br>Please refer to the prompt messages included in the CLI interface.   |      |

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

- ACL** (Access Control List Configuration)
- CFM** (Connectivity Fault Management Configuration)
- CM** (Class Map Configuration)
- ERPS** (Ethernet Ring Protection Switching 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)



## 3

# General Commands

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

**Table 7: General Commands**

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

**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: 255 characters)

### Default Setting

Console

**Command Mode**

Global Configuration

**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 | weekly day-of-week |
monthly day}] | 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: 0-59)

**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-week* - Day of the week at which to reload. (Range: monday ... saturday)

*day* - Day of the month at which to reload. (Range: 1-31)

**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 115).

### 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 74.

### Syntax

**enable** [*level*]

*level* - Privilege level to log into the device. (Range: 15)

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 \(88\)](#)

[enable password \(216\)](#)

**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

Press ENTER to start session

User Access Verification

Username:
```

**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 74](#).

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```

Console#configure
Console(config)#

```

**Related Commands**

[end \(89\)](#)

**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 74](#).

**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 \(85\)](#)

**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
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

## 4

# 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**

| Command Group                        | Function   |
|--------------------------------------|--|
| <a href="#">Device Designation</a>   | Configures information that uniquely identifies this switch  |
| <a href="#">Banner Information</a>   | Configures administrative contact, device identification and location                                      |
| <a href="#">System Status</a>        | Displays system configuration, active managers, and version information                                    |
| <a href="#">Frame Size</a>           | Enables support for jumbo frames   |
| <a href="#">File Management</a>      | Manages code image or switch configuration files   |
| <a href="#">Line</a>                 | Sets communication parameters for the serial port, including baud rate and console time-out                |
| <a href="#">Event Logging</a>        | Controls logging of error messages   |
| <a href="#">SMTP Alerts</a>          | Configures SMTP email alerts   |
| <a href="#">Time (System Clock)</a>  | Sets the system clock automatically via NTP/SNTP server or manually  |
| <a href="#">Time Range</a>           | Sets a time range for use by other functions, such as Access Control Lists                                 |
| <a href="#">Synchronous Ethernet</a> | Synchronizes specified links to the same frequency in order to transfer timing information to remote sites |
| <a href="#">Switch Clustering</a>    | Configures management of multiple devices via a single IP address  |

## Device Designation

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

**Table 9: Device Designation Commands**

| Command                              | Function                               | Mode |
|--------------------------------------|--|------|
| <a href="#">hostname</a>             | Specifies the host name for the switch | GC   |
| <a href="#">snmp-server contact</a>  | Sets the system contact string         | GC   |
| <a href="#">snmp-server location</a> | Sets the system location string        | GC   |

**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

### Example

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

---

## Banner Information

These commands are used to configure and manage administrative information about the switch, its exact data center location, details of the electrical and network circuits that supply the switch, as well as contact information for the network administrator and system manager. This information is only available via the CLI and is automatically displayed before login as soon as a console or telnet connection has been established.

**Table 10: Banner Commands**

| Command   | Function  | Mode |
|---|---|------|
| <a href="#">banner configure</a>                    | Configures the banner information that is displayed before login          | GC   |
| <a href="#">banner configure company</a>            | Configures the Company information that is displayed by banner            | GC   |
| <a href="#">banner configure dc-power-info</a>      | Configures the DC Power information that is displayed by banner           | GC   |
| <a href="#">banner configure department</a>         | Configures the Department information that is displayed by banner         | GC   |
| <a href="#">banner configure equipment-info</a>     | Configures the Equipment information that is displayed by banner          | GC   |
| <a href="#">banner configure equipment-location</a> | Configures the Equipment Location information that is displayed by banner | GC   |
| <a href="#">banner configure ip-lan</a>             | Configures the IP and LAN information that is displayed by banner         | GC   |

Table 10: Banner Commands (Continued)

| Command                                    | Function   | Mode   |
|--|--|--------|
| <code>banner configure lp-number</code>    | Configures the LP Number information that is displayed by banner                         | GC     |
| <code>banner configure manager-info</code> | Configures the Manager contact information that is displayed by banner                   | GC     |
| <code>banner configure mux</code>          | Configures the MUX information that is displayed by banner                               | GC     |
| <code>banner configure note</code>         | Configures miscellaneous information that is displayed by banner under the Notes heading | GC     |
| <code>show banner</code>                   | Displays all banner information  | NE, PE |

**banner configure** This command is used to interactively specify administrative information for this device.

### Syntax

```
banner configure
```

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

The administrator can batch-input all details for the switch with one command. When the administrator finishes typing the company name and presses the enter key, the script prompts for the next piece of information, and so on, until all information has been entered. Pressing enter without inputting information at any prompt during the script's operation will leave the field empty. Spaces can be used during script mode because pressing the enter key signifies the end of data input. The delete and left-arrow keys terminate the script. The use of the backspace key during script mode is not supported. If, for example, a mistake is made in the company name, it can be corrected with the **banner configure company** command.

### Example

```
Console(config)#banner configure

Company: Edge-Core Networks
Responsible department: R&D Dept
Name and telephone to Contact the management people
Manager1 name: Sr. Network Admin
phone number: 123-555-1212
Manager2 name: Jr. Network Admin
phone number: 123-555-1213
Manager3 name: Night-shift Net Admin / Janitor
phone number: 123-555-1214
```

```
The physical location of the equipment.  
City and street address: 12 Straight St. Motown, Zimbabwe  
Information about this equipment:  
Manufacturer: Edge-Core Networks  
ID: 123_unique_id_number  
Floor: 2  
Row: 7  
Rack: 29  
Shelf in this rack: 8  
Information about DC power supply.  
Floor: 2  
Row: 7  
Rack: 25  
Electrical circuit: : ec-177743209-xb  
Number of LP:12  
Position of the equipment in the MUX:1/23  
IP LAN:192.168.1.1  
Note: This is a random note about this managed switch and can contain  
miscellaneous information.  
Console(config)#
```

**banner configure company** This command is used to configure company information displayed in the banner. Use the **no** form to remove the company name from the banner display.

#### Syntax

**banner configure company** *name*

**no banner configure company**

*name* - The name of the company.  
(Maximum length: 32 characters)

#### Default Setting

None

#### Command Mode

Global Configuration

#### Command Usage

Input strings cannot contain spaces. The **banner configure company** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

#### Example

```
Console(config)#banner configure company Big-Ben  
Console(config)#
```

**banner configure dc-power-info** This command is use to configure DC power information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

```
banner configure dc-power-info floor floor-id row row-id  
rack rack-id electrical-circuit ec-id
```

```
no banner configure dc-power-info [floor | row | rack |  
electrical-circuit]
```

*floor-id* - The floor number.

*row-id* - The row number.

*rack-id* - The rack number.

*ec-id* - The electrical circuit ID.

Maximum length of each parameter: 32 characters

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure dc-power-info** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure dc-power-info floor 3 row 15 rack 24  
    electrical-circuit 48v-id_3.15.24.2  
Console(config)#
```

**banner configure department** This command is used to configure the department information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

```
banner configure department dept-name
```

```
no banner configure department
```

*dept-name* - The name of the department.  
(Maximum length: 32 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure department** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure department R&D
Console(config)#
```

**banner configure equipment-info** This command is used to configure the equipment information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

**banner configure equipment-info manufacturer-id** *mfr-id*  
**floor** *floor-id* **row** *row-id* **rack** *rack-id* **shelf-rack** *sr-id* **manufacturer**  
*mfr-name*

**no banner configure equipment-info** [**floor** | **manufacturer** |  
**manufacturer-id** | **rack** | **row** | **shelf-rack**]

*mfr-id* - The name of the device model number.

*floor-id* - The floor number.

*row-id* - The row number.

*rack-id* - The rack number.

*sr-id* - The shelf number in the rack.

*mfr-name* - The name of the device manufacturer.

Maximum length of each parameter: 32 characters

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure equipment-info** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure equipment-info manufacturer-id ECS4810-12M
  floor 3 row 10 rack 15 shelf-rack 12 manufacturer Edge-Core
Console(config)#
```

**banner configure equipment-location** This command is used to configure the equipment location information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

**banner configure equipment-location** *location*

**no banner configure equipment-location**

*location* - The address location of the device.  
(Maximum length: 32 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure equipment-location** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure equipment-location
  710_Network_Path,_Indianapolis
Console(config)#
```

**banner configure ip-lan** This command is used to configure the device IP address and subnet mask information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

**banner configure ip-lan** *ip-mask*

**no banner configure ip-lan**

*ip-mask* - The IP address and subnet mask of the device.  
(Maximum length: 32 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure ip-lan** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure ip-lan 192.168.1.1/255.255.255.0  
Console(config)#
```

**banner configure ip-number** This command is used to configure the LP number information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

**banner configure ip-number** *lp-num*

**no banner configure ip-number**

*lp-num* - The LP number. (Maximum length: 32 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure ip-number** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure lp-number 12  
Console(config)#
```

**banner configure manager-info** This command is used to configure the manager contact information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

```
banner configure manager-info
name mgr1-name phone-number mgr1-number
[name2 mgr2-name phone-number mgr2-number |
name3 mgr3-name phone-number mgr3-number]
no banner configure manager-info [name1 | name2 / name3]
```

*mgr1-name* - The name of the first manager.

*mgr1-number* - The phone number of the first manager.

*mgr2-name* - The name of the second manager.

*mgr2-number* - The phone number of the second manager.

*mgr3-name* - The name of the third manager.

*mgr3-number* - The phone number of the third manager.

Maximum length of each parameter: 32 characters

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure manager-info** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure manager-info name Albert_Einstein phone-
number 123-555-1212 name2 Lamar phone-number 123-555-1219
Console(config)#
```

**banner configure mux** This command is used to configure the mux information displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

```
banner configure mux muxinfo
```

```
no banner configure mux
```

*muxinfo* - The circuit and PVC to which the switch is connected.  
(Maximum length: 32 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure mux** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure mux telco-8734212kx_PVC-1/23  
Console(config)#
```

**banner configure note** This command is used to configure the note displayed in the banner. Use the **no** form to restore the default setting.

### Syntax

**banner configure note** *note-info*

**no banner configure note**

*note-info* - Miscellaneous information that does not fit the other banner categories, or any other information of importance to users of the switch CLI. (Maximum length: 150 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

Input strings cannot contain spaces. The **banner configure note** command interprets spaces as data input boundaries. The use of underscores ( `_` ) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

### Example

```
Console(config)#banner configure note !!!!!ROUTINE_MAINTENANCE_firmware-  
upgrade_0100-0500_GMT-0500_20071022!!!!!!_20min_network_impact_expected  
Console(config)#
```

**show banner** This command displays all banner information.

### Command Mode

Normal Exec, Privileged Exec

### Example

```

Console#show banner
Edge-Core
WARNING - MONITORED ACTIONS AND ACCESSES
R&D

Albert_Einstein - 123-555-1212
Lamar - 123-555-1219

Station's information:
710_Network_Path,_Indianapolis

Edge-Core - ECS4810-12M
Floor / Row / Rack / Sub-Rack
3/ 10 / 15 / 12
DC power supply:
Power Source A: Floor / Row / Rack / Electrical circuit
3/ 15 / 24 / 48v-id_3.15.24.2
Number of LP: 12
Position MUX: telco-8734212kx_PVC-1/23
IP LAN: 192.168.1.1/255.255.255.0
Note: !!!!!ROUTINE_MAINTENANCE_firmware-upgrade_0100-0500_GMT-
0500_20071022!!!!!!_20min_network_
Console#

```

## System Status

This section describes commands used to display system information.

**Table 11: System Status Commands**

| Command  | Function   | Mode   |
|--|--|--------|
| <a href="#">show access-list</a><br><a href="#">tcam-utilization</a> | Shows utilization parameters for TCAM  | PE     |
| <a href="#">show alarm</a>   | Shows the name assigned to the predefined alarms   | PE     |
| <a href="#">show alarm-status</a>                                    | Shows information for predefined alarms  | PE     |
| <a href="#">show memory</a>  | Shows memory utilization parameters  | NE, PE |
| <a href="#">show process cpu</a>                                     | Shows CPU utilization parameters   | NE, PE |
| <a href="#">show process cpu guard</a>                               | Shows the CPU utilization watermark and threshold  | NE     |
| <a href="#">show running-config</a>                                  | Displays the configuration data currently in use   | PE     |
| <a href="#">show startup-config</a>                                  | Displays the contents of the configuration file (stored in flash memory) that is used to start up the system | PE     |
| <a href="#">show system</a>  | Displays system information  | NE, PE |

Table 11: System Status Commands (Continued)

| Command                        | Function  | Mode   |
|--------------------------------|---|--------|
| <code>show tech-support</code> | Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems | PE     |
| <code>show users</code>        | Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients              | NE, PE |
| <code>show version</code>      | Displays version information for the system   | NE, PE |
| <code>show watchdog</code>     | Shows if watchdog debugging is enabled  | PE     |
| <code>watchdog software</code> | Monitors key processes, and automatically reboots the system if any of these processes are not responding correctly         | PE     |

**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, and the overall percentage of TCAM in use.

**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
Total Policy Control Entries : 1024
Free Policy Control Entries  : 1016
Entries Used by System      : 118
Entries Used by User        : 4294967186
TCAM Utilization            : 0.78%
Console#
```

**show alarm** This command shows the name assigned to the predefined alarms.

#### Syntax

**show alarm input name *unit alarm-input-index***

*unit* - The parameter only applies to stackable switches. (Range: 1)

*alarm-input-index* - Index of signal on the Alarm Input port.  
(Range: 1-4)

## Command Mode

Privileged Exec

## Command Usage

The alarms supported by this switch include various external alarms which can be sent to the switch through hard-wired connections described in the *Installation Guide*. Refer to the *Installation Guide* for information on how to use the alarm relay contacts and external site alarm inputs.

## Example

```
Console#show alarm input name
Name of Alarm Input of unit 1 index 1:
  ALARM_IN1
Name of Alarm Input of unit 1 index 2:
  ALARM_IN2
Name of Alarm Input of unit 1 index 3:
  ALARM_IN3
Name of Alarm Input of unit 1 index 4:
  ALARM_IN4
Console#
```

**show alarm-status** This command displays information on predefined alarms (i.e., non-configurable) and on the link-down alarm (which is displayed as a minor alarm).

## Command Mode

Privileged Exec

## Command Usage

- ◆ Alarms are signalled through the Alarm LEDs (Major Alarm and Minor Alarm) and the Alarm Input and Output port on the front panel. When an alarm occurs, the corresponding LEDs will not be extinguished until the alarm condition is resolved. The event that triggered the alarm can be viewed using this command. Alarms are also recorded in the system log, and can viewed using the [show log](#) command.
- ◆ The alarms supported by this switch include the internal alarms described below and various external alarms which can be sent to the switch through hard-wired connections described in the *Installation Guide*. Refer to the *Installation Guide* for information on how to use the alarm relay contacts and external site alarm inputs.
- ◆ Major alarms include the failure of all fans, both thermal detectors exceeding 65°C, or an invalid power module being installed. Minor alarms include the failure of one or two fans, or when a second power module is installed but it is not functioning.

### Example

The following shows the message types displayed when no alarms are active, and another example when both minor and major alarms occur.

```
Console#show alarm-status
Unit 1
  Asserted Alarm Input   : [NONE]
  Current Major Alarm Status:[NONE]
  Current Minor Alarm Status:[NONE]
  Current Major Alarm Output Status:[INACTIVE]
  Current Minor Alarm Output Status:[INACTIVE]
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, and the total amount of system memory.

### Example

```
Console#show memory
Status Bytes      %
-----
Free      30994432  23
Used     103223296  77
Total    134217728

Alarm Configuration
Rising Threshold      : 90%
Falling Threshold     : 80%

Console#
```

### Related Commands

[memory \(196\)](#)

**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 : 23%
```

```

CPU Utilization in the past 60 seconds
Average Utilization      : 23%
Maximum Utilization     : 28%

Alarm Status
Current Alarm Status    : Off
Last Alarm Start Time   : Oct  4 09:45:45 2013
Last Alarm Duration Time : 10 seconds

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

Console#

```

## Related Commands

[process cpu \(197\)](#)

**show process cpu guard** This command shows the CPU utilization watermark and threshold settings.

**Command Mode**  
Normal Exec, Privileged Exec

### Example

```

Console#show process cpu guard
CPU Guard Configuration
Status          : Disabled
High Watermark  : 90%
Low Watermark   : 70%
Maximum Threshold : 500 packets per second
Minimum Threshold : 50 packets per second
Trap Status     : Disabled
CPU Guard Operation
Current Threshold : 500 packets per second

Console#

```

**Table 12: show process cpu guard - display description**

| Field                          | Description   |
|--------------------------------|---|
| <i>CPU Guard Configuration</i> |   |
| Status                         | Shows if CPU Guard has been enabled.  |
| High Watermark                 | If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark.   |
| Low Watermark                  | If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark.   |
| Maximum Threshold              | If the number of packets being processed by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold. |

Table 12: show process cpu guard - display description

| Field                      | Description  |
|----------------------------|--|
| Minimum Threshold          | If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold. |
| Trap Status                | Shows if an alarm message will be generated when utilization exceeds the high watermark or exceeds the maximum threshold.                            |
| <i>CPU Guard Operation</i> |  |
| Current Threshold          | Shows the configured threshold in packets per second.  |

### Related Commands

[process cpu guard \(212\)](#)

**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: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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 server settings
  - 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
- Layer 4 precedence settings
- Spanning tree settings
- Interface settings
- Any configured settings for the console port and Telnet

### Example

```

Console#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_00</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
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
VLAN 1 name DefaultVlan media ethernet state active
VLAN 4093 media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
switchport allowed vlan add 4093 tagged
:
!
interface vlan 1
ip address dhcp
!
interface craft
!
line console
!
line vty
!
end
!
Console#

```

### Related Commands

[show startup-config \(108\)](#)

**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
  - RMON alarms settings
  - 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 \(106\)](#)

**show system** This command displays system information.

#### Default Setting

None

#### Command Mode

Normal Exec, Privileged Exec

#### Command Usage

- ◆ For a description of the items shown by this command, refer to "Displaying System Information" in the *Web Management Guide*.
- ◆ If any POST test indicates “FAIL,” contact your distributor for assistance.

### Example

```
Console#show system
System Description : ECS4810-12M
System OID String  : 1.3.6.1.4.1.259.10.1.11
System Information
  System Up Time      : 0 days, 3 hours, 11 minutes, and 23.2 seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 70-72-CF-1C-BA-52
  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

  Main Power Status   : Active
  Redundant Power Status : Inactive
Console#
```

**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

show system:
System Description : ECS4810-12M
System OID String  : 1.3.6.1.4.1.259.10.1.11
System Information
  System Up Time      : 0 days, 3 hours, 11 minutes, and 23.2 seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 70-72-CF-1C-BA-52
  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

  Main Power Status   : Active
  Redundant Power Status : Inactive
.
```

:

**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   User Name                Idle time (h:m:s) Remote IP addr
  -----
  console admin                0:14:14
  * VTY 0 admin                0:00:00   192.168.1.19
  SSH 1  steve                    0:00:06   192.168.1.19

Web Online Users:
  Line   User Name                Idle time (h:m:s) Remote IP Addr
  -----
  HTTP  admin                0:00:00   192.168.1.19

Console#
```

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

### Command Mode

Normal Exec, Privileged Exec

### Command Usage

See "Displaying Hardware/Software Versions" in the *Web Management Guide* for detailed information on the items displayed by this command.

### Example

```
Console#show version
Unit 1
Unit 1
  Serial Number      : S123456
  Hardware Version   : R0B
  EPLD Version       : 0.00
  Number of Ports    : 12
  Main Power Status  : Active
  Redundant Power Status : Inactive
  Role               : Master
  Loader Version     : 1.0.0.8
  Linux Kernel Version : 2.6.22.18
  Boot ROM Version   : 1.0.0.0
  Operation Code Version : 1.1.4.10

Console#
```

**show watchdog** This command shows if watchdog debugging is enabled.

**Command Mode**  
Privileged Exec

### Example

```
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#watchdog
Console#
```

## Frame Size

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

**Table 13: Frame Size Commands**

| Command                     | Function                         | Mode |
|-----------------------------|----------------------------------|------|
| <a href="#">jumbo frame</a> | Enables support for jumbo frames | GC   |

**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**

| Command                                | Function  | Mode |
|--|---|------|
| <i>General Commands</i>                |   |      |
| <code>boot system</code>               | Specifies the file or image used to start up the system   | GC   |
| <code>copy</code>                      | Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server     | PE   |
| <code>delete</code>                    | Deletes a file or code image  | PE   |
| <code>dir</code>                       | Displays a list of files in flash memory  | PE   |
| <code>whichboot</code>                 | Displays the files booted   | PE   |
| <i>Automatic Code Upgrade Commands</i> |   |      |
| <code>upgrade opcode auto</code>       | Automatically upgrades the current image when a new version is detected on the indicated server | GC   |
| <code>upgrade opcode path</code>       | Specifies an FTP/TFTP server and directory in which the new opcode is stored                    | GC   |
| <code>upgrade opcode reload</code>     | Reloads the switch automatically after the opcode upgrade is completed                          | GC   |
| <code>show upgrade</code>              | Shows the opcode upgrade configuration settings.  | PE   |
| <i>TFTP Configuration Commands</i>     |   |      |

Table 14: Flash/File Commands (Continued)

| Command                         | Function  | Mode |
|---------------------------------|---|------|
| <a href="#">ip tftp retry</a>   | Specifies the number of times the switch can retry transmitting a request to a TFTP server  | GC   |
| <a href="#">ip tftp timeout</a> | 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 | GC   |

## 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 \(119\)](#)

[whichboot \(120\)](#)

**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 running-config {file | ftp | startup-config | tftp}**

**copy startup-config {file | ftp | running-config | tftp}**

**copy tftp {file | https-certificate | public-key | running-config | startup-config}**

**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 242.)

**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 *Web Management 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: <1-2>: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

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: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

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

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
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]:
Write to FLASH Programming.

\Write to FLASH finish.
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* | **public-key** *username* [**dsa** | **rsa**] }

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

**public-key** - Keyword that allows you to delete a SSH key on the switch. (See “Secure Shell” on page 242.)

*username* – Name of an SSH user. (Range: 1-8 characters)

**dsa** – DSA public key type.

**rsa** – RSA public key type.

### 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.
- ◆ If the public key type is not specified, then both DSA and RSA keys will be deleted.

### Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg  
Console#
```

### Related Commands

[dir \(119\)](#)

[delete public-key \(247\)](#)

**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**

| Column Heading | Description  |
|----------------|--|
| File Name      | The name of the file.                                  |
| File Type      | File types: Boot-Rom, Operation Code, and Config file. |
| Startup        | Shows if this file is used when the system is started. |
| Create Time    | The date and time the file was created.                |
| Size           | The length of the file in bytes.                       |

### Example

The following example shows how to display all file information:

```

Console#dir
      File Name                Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
ecs4810_12m_1.1.2.2.bix       OpCode  N    2013-10-07 11:09:12    12933584
ecs4810_12m_v1.1.4.10.bix    OpCode  Y    2012-10-19 08:12:39    12982728
Factory_Default_Config.cfg    Config  N    2012-02-02 06:05:21      455
startup1.cfg                  Config  Y    2013-10-04 09:46:01     1165
-----
Free space for compressed user config files: 626688
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#whichboot
File Name                               Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
ecs4810_12m_v1.1.4.10.bix              OpCode   Y    2012-10-19 08:12:39    12982728
startup1.cfg                            Config   Y    2013-10-04 09:46:01      1165
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 `ecs-runtime.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(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 bootstrap.

```
:
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
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**

*opcode-dir-url* - 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 `ecs-runtime.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://admin: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   : ecs3510-28t.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**

*seconds* - The 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)#
```

## Line

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**

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

\* 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)#
```

#### Related Commands

[show line \(135\)](#)

[show users \(110\)](#)

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

### Related Commands

[parity \(129\)](#)

**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: 0 - 65535 seconds; 0: no timeout)

### Default Setting

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)#exec-timeout 120
Console(config-line)#
```

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

### Related Commands

[username \(217\)](#)

[password \(129\)](#)

**parity** This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

### Syntax

**parity** { **none** | **even** | **odd** }

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

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

### Syntax

**password** { **0** | **7** } *password*

**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 an FTP server. There is no need for you to manually configure encrypted passwords.

#### Example

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

#### Related Commands

[login \(128\)](#)

[password-thresh \(130\)](#)

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

### Related Commands

[silent-time \(131\)](#)

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

### Related Commands

[password-thresh \(130\)](#)

**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.

### Example

To specify 57600 bps, enter this command:

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

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

**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)#timeout login response 120
Console(config-line)#
```

**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 \(251\)](#)[show users \(110\)](#)

**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: 0-512, 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
  Silent Time        : Disabled
  Baud Rate          : 115200
  Data Bits          : 8
  Parity              : None
  Stop Bits          : 1

VTY Configuration:
  Password Threshold : 3 times
  EXEC Timeout       : 600 seconds
  Login Timeout      : 300 sec.
  Silent Time        : Disabled
Console#
```

## Event Logging

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

**Table 17: Event Logging Commands**

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

**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
Console(config)#
```

**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**

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

### 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* - The UDP port number used by the remote server.  
(Range: 1-65535)

#### Default Setting

UPD Port: 514

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

### Related Commands

[logging history \(137\)](#)

[logging trap \(139\)](#)

[clear log \(140\)](#)

**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 137](#). 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 \(140\)](#)

**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 146](#)).

**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#
```

**Table 19: show logging flash/ram - display description**

| Field                    | Description  |
|--------------------------|--|
| Syslog logging           | Shows if system logging has been enabled via the <a href="#">logging on</a> command. |
| History logging in FLASH | The message level(s) reported based on the <a href="#">logging history</a> command.  |
| History logging in RAM   | The message level(s) reported based on the <a href="#">logging history</a> command.  |

The following example displays settings for the trap function.

```
Console#show logging trap
Remote Log Status           : Disabled
Remote Log Facility Type    : Local use 7
Remote Log Level Type       : Debugging messages
Remote Log Server IP Address : 0.0.0.0
Console#
```

**Table 20: show logging trap - display description**

| Field                        | Description  |
|------------------------------|--|
| Remote Log Status            | Shows if remote logging has been enabled via the <a href="#">logging trap</a> command.                                       |
| Remote Log Facility Type     | The facility type for remote logging of syslog messages as specified in the <a href="#">logging facility</a> command.        |
| Remote Log Level Type        | The severity threshold for syslog messages sent to a remote server as specified in the <a href="#">logging trap</a> command. |
| Remote Log Server IP Address | The address of syslog servers as specified in the <a href="#">logging host</a> command.                                      |

### Related Commands

[show logging sendmail \(146\)](#)

## 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**

| Command                                | Function  | Mode |
|--|---|------|
| <a href="#">logging sendmail</a>       | Enables SMTP event handling                       | GC   |
| <a href="#">logging sendmail host</a>  | SMTP servers to receive alert messages            | GC   |
| <a href="#">logging sendmail level</a> | Severity threshold used to trigger alert messages | GC   |

**Table 21: Event Logging Commands** (Continued)

| Command   | Function  | Mode   |
|---|---|--------|
| <code>logging sendmail destination-email</code> | Email recipients of alert messages                    | GC     |
| <code>logging sendmail source-email</code>      | Email address used for "From" field of alert messages | GC     |
| <code>show logging sendmail</code>              | Displays SMTP event handler settings                  | NE, PE |

**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 or IPv6 address of an SMTP server that will be sent alert messages for event handling.

**Default Setting**

None

**Command Mode**

Global Configuration

**Command Usage**

- ◆ You can specify up to three SMTP servers for event handling. 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**

*level* - One of the system message levels ([page 137](#)). 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**

| Command                                     | Function  | Mode   |
|---|---|--------|
| <i>SNTP Commands</i>                        |   |        |
| <code>sntp client</code>                    | Accepts time from specified time servers                | GC     |
| <code>sntp poll</code>                      | Sets the interval at which the client polls for time    | GC     |
| <code>sntp server</code>                    | Specifies one or more time servers                      | GC     |
| <code>show sntp</code>                      | Shows current SNTP configuration settings               | NE, PE |
| <i>Manual Configuration Commands</i>        |   |        |
| <code>clock summer-time (date)</code>       | Configures summer time* for the switch's internal clock | GC     |
| <code>clock summer-time (predefined)</code> | Configures summer time* for the switch's internal clock | GC     |
| <code>clock summer-time (recurring)</code>  | Configures summer time* for the switch's internal clock | GC     |
| <code>clock timezone</code>                 | Sets the time zone for the switch's internal clock      | GC     |
| <code>calendar set</code>                   | Sets the system date and time                           | PE     |
| <code>show calendar</code>                  | Displays the current date and time setting              | NE, PE |

\* Daylight savings time.

## SNTP Commands

**sntp client** This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the [sntp server](#) command. Use the **no** form to disable SNTP client requests.

### Syntax

[no] **sntp 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 (i.e., 00:00:00, Jan. 1, 2001).
- ◆ This command enables client time requests to time servers specified via the [sntp server](#) command. 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(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 \(148\)](#)

[sntp poll \(148\)](#)

[show sntp \(149\)](#)

**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

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

### Related Commands

[sntp client \(147\)](#)

**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* - IPv4 or IPv6 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)#ntp server 10.1.0.19
Console#
```

### Related Commands

[ntp client \(147\)](#)

[ntp poll \(148\)](#)

[show ntp \(149\)](#)

**show ntp** 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 ntp
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#
```

## 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-year 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: 0-99 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 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 time zone deviates from your regular time zone (that is, the offset).

### Example

The following example sets the 2014 Summer Time ahead by 60 minutes on March 9th and returns to normal time on November 2nd.

```
Console(config)#clock summer-time DEST date march 9 2014 01 59 november 2
2014 01 59 60
Console(config)#
```

**Related Commands**[show sntp \(149\)](#)

**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**

*name* - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

**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 \(recurring\)](#)).

**Table 23: Predefined Summer-Time Parameters**

| Region      | Start Time, Day, Week, & Month      | End Time, Day, Week, & Month         | Rel. Offset |
|-------------|-------------------------------------|--------------------------------------|-------------|
| Australia   | 00:00:00, Sunday, Week 5 of October | 23:59:59, Sunday, Week 5 of March    | 60 min      |
| Europe      | 00:00:00, Sunday, Week 5 of March   | 23:59:59, Sunday, Week 5 of October  | 60 min      |
| New Zealand | 00:00:00, Sunday, Week 1 of October | 23:59:59, Sunday, Week 3 of March    | 60 min      |
| USA         | 00:00:00, Sunday, Week 2 of March   | 23:59:59, Sunday, Week 1 of November | 60 min      |

**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
Console(config)#
```

**Related Commands**

[show sntp \(149\)](#)

**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**)

*b-month* - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **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: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

*e-month* - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **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: 0-99 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 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).

### 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 Sunday of the 2nd week of November at 01:59 hours.

```
Console(config)#clock summer-time MESZ recurring 1 friday june 23 59 3
saturday september 2 55 60
Console(config)#
```

### Related Commands

[show sntp \(149\)](#)

**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)

*hours* - 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 (east) of UTC.

**after-utc** - Sets the local time zone after (west) 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 (before) or west (after) of UTC.

### Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

### Related Commands

[show sntp \(149\)](#)

**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)

*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, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

**show calendar** This command displays the system clock.

### Default Setting

None

### Command Mode

Normal Exec, Privileged Exec

### Example

```
Console#show calendar
Current Time       : Mar  6 20:22:05 2014
Time Zone         : UTC, 00:00
Summer Time       : Not configured
Summer Time in Effect : No
Console#
```

## Time Range

This section describes the commands used to sets a time range for use by other functions, such as Access Control Lists.

**Table 24: Time Range Commands**

| Command                         | Function   | Mode |
|---------------------------------|--|------|
| <a href="#">time-range</a>      | Specifies the name of a time range, and enters time range configuration mode | GC   |
| <a href="#">absolute</a>        | Sets the time range for the execution of a command                           | TR   |
| <a href="#">periodic</a>        | Sets the time range for the periodic execution of a command                  | TR   |
| <a href="#">show time-range</a> | Shows configured time ranges.  | PE   |

**time-range** This command specifies the name of a time range, and enters time range configuration mode. Use the **no** form to remove a previously specified time range.

### 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.

### Example

```
Console(config)#time-range r&d  
Console(config-time-range)#
```

### Related Commands

[Access Control Lists \(343\)](#)

**absolute** This command sets the 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: 2009-2109)

### 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 (i.e., 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

```
[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

*hour* - Hour in 24-hour format. (Range: 0-23)

*minute* - 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 (i.e., 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#
```

---

## Synchronous Ethernet

Synchronous Ethernet (SyncE) is used to synchronize specified links to the same frequency in order to transfer timing information to remote sites. SyncE ensures that all nodes have a clock source traceable to a Primary Reference Clock (PRC). The commands described in this section are used to enable SyncE on specified interfaces, automatically or manually select a clock source, receive Synchronization Status Messages (SSM) used to select the clock source based on the indicated quality level.

Table 25: Sync-E Commands

| Command  | Function  | Mode |
|--|---|------|
| <code>syncce</code>                              | Enables SyncE on all ports that support SyncE   | GC   |
| <code>syncce ethernet</code>                     | Enables SyncE on a port that supports SyncE   | GC   |
| <code>syncce ethernet clock-source</code>        | Manually sets a port as a clock source or candidate clock source at the specified priority                              | GC   |
| <code>syncce auto-clock-source-selecting</code>  | Automatically selects the clock-source port with the highest priority   | GC   |
| <code>syncce force-clock-source-selecting</code> | Sets the local clock as the active clock source, or sets a port to be the active clock source                           | GC   |
| <code>syncce ssm ethernet</code>                 | Configures a port to receive/send SSM messages, and sets the priority used for this port in clock source port selection | GC   |
| <code>syncce clk-src-ssm</code>                  | Uses SSM to select the clock source according to the SSM quality level, priority and port number                        | GC   |
| <code>show syncce</code>                         | Shows SyncE status, selection mode, clock source status, and SSM status   | PE   |

**syncce** This command enables SyncE on all ports that support SyncE. Use the **no** form to disable SyncE on all ports that support SyncE.

### Syntax

**[no] syncce**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ This command enables SyncE on ports 25-28. It does not configure any of these port to be the clock source.
- ◆ SyncE must be enabled on a port before the clock selection method can be set. Selection options include manual (`syncce ethernet clock-source`), automatic (`syncce auto-clock-source-selecting`), or forced (`syncce force-clock-source-selecting`).
- ◆ SyncE frequency synchronization uses physical layer Ethernet to distribute timing information. A synchronization chain is formed by using a stratum 1 traceable source at one end which is then recovered at downstream PHYs and retransmitted down the chain. Every node in the chain must be capable of recovering and re-transmitting frequency synchronization signals.
- ◆ SyncE provides timing synchronization through the physical layer, while PTP (Precision Time Protocol) uses a higher level packet protocol which can result in

processing delays. However, both SyncE and PTP may be used in combination to achieve a high level of frequency synchronization with a common defined time.

- ◆ SyncE delivers a high level of frequency accuracy, but cannot deliver time-of-day information (i.e., GMT). Conversely, PTP supports time-of-day information required by billing and service level agreements.
- ◆ SyncE implementation guidelines are covered by these standards:

**Table 26: Synchronous Ethernet Standards**

| Standard          | Description  |
|-------------------|--|
| ITU G.8264/Y.1364 | Distribution of timing information through packet networks             |
| ITU G.8261/Y.1361 | Timing and synchronization aspects in packet networks                  |
| ITU G.8262/Y.1362 | Timing characteristics of a synchronous Ethernet equipment slave clock |

### Example

```
Console(config)#sync e
Console(config)#exit
Console#show sync e
SyncE Status:
Port          Status      Clock Source
-----
Eth 1/ 9     Enabled    No
Eth 1/10     Enabled    No
Eth 1/11     Enabled    No
Eth 1/12     Enabled    No
...
```

**sync e ethernet** This command enables SyncE on a port that supports SyncE. Use the **no** form to disable SyncE on a port.

### Syntax

**[no] sync e ethernet *unit/port***  
*unit* - Unit identifier. (Range: 1)  
*port* - Port number. (Range: 1-12)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ This command only enables SyncE on the specified port. It does not configure the port to be the clock source.

- ◆ This command can enable SyncE on trunk member but not on a trunk.
- ◆ SyncE can only be enabled on two ports at the same time.

### Example

```
Console(config)#syncd ethernet 1/28  
Console(config)#
```

**synce ethernet clock-source** This command manually sets a port as a clock source, or as a candidate clock source at the specified priority when using automatic clock source selection. Use the **no** form to remove a port as a clock source.

### Syntax

**synce ethernet *unit/port* clock-source [*priority* *priority*]**

**no synce ethernet *unit/port* clock-source**

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*priority* - The priority used by automatic clock source selection.  
(Range: 1-65535)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ This command can enable SyncE on trunk member but not on a trunk.
- ◆ If more than one port is configured as clock source port with this command, the first configured port will be set as the active clock source port.
- ◆ If an active clock source port is removed as the clock source, no active clock source port will exist until explicitly configured.
- ◆ When no active clock-source port exists, the switch's internal clock will be used as the clock source.
- ◆ If the priority of the clock-source port is not specified, the port ID of the clock-source port will be used as the priority for automatic clock source selection (see the [synce auto-clock-source-selecting](#) command).
- ◆ Lower priority values indicate higher precedence. If more than two clock-source ports have the same priority value, the clock source-port with the lowest port ID assumes higher precedence.

- ◆ If SyncE has locked the clock source and the clock source becomes invalid, SyncE will operate in holdover mode, switching over to the local reference clock if all available clock source signals fail. If SyncE has never locked the clock source and no valid clock source exists, SyncE will operate in free-run mode. If SyncE locked the clock source, SyncE will operate in locked mode.

Note that a clock is said to be in holdover mode if it was previously synchronized to another clock (normally the primary reference clock) but is now free-running on its own internal oscillator, whose frequency is being adjusted using data acquired while it had been synchronized to the other clock.

### Example

```
Console(config)#sync e ethernet 1/25 clock-source priority 1
Console(config)#
```

**sync e auto-clock-source-selecting** This command automatically selects the clock source port with the highest priority. Use the **no** form to disable automatic clock source selection.

### Syntax

**[no] sync e auto-clock-source-selecting [revertive-switching]**

**auto-clock-source-selecting** - Chooses the clock source port based on current clock-source port status and priority.

**revertive-switching** - The active clock source port will be changed when a clock source port with a higher priority becomes available.

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ The switch can only be set to automatic clock source selection mode when the current selection mode is set to manual.
- ◆ At least one clock source port must be configured before switching to auto clock source selection mode. All ports configured as clock source port in manual mode will be kept after changing to auto mode.
- ◆ If more than one port is configured as clock source port, the port with a valid clock source signal and the highest priority is selected to be the active clock source port.
- ◆ If the configured priorities for two or more clock source ports are the same, it will choose the smaller numbered port to be the active clock source port.

- ◆ If revertive switching is enabled, the active clock source port will be changed when a clock source port with a higher priority becomes available. If revertive switching is disabled, the active clock source port will not be changed unless the current active clock source becomes invalid.
- ◆ If SyncE has locked the clock source and the clock source becomes invalid, SyncE will operate in holdover mode, switching over to the local reference clock if all available clock source signals fail. If SyncE has never locked the clock source and no valid clock source exists, SyncE will operate in free-run mode. If SyncE locked the clock source, SyncE will operate in locked mode.

### Example

```

Console(config)#sync e auto-clock-source-selecting revertive-switching
Console(config)#end
Console#show sync e
SyncE Status:
Port          Status      Clock Source
-----
Eth 1/ 9      Enabled    Yes
Eth 1/10      Disabled   No
Eth 1/11      Disabled   No
Eth 1/12      Disabled   No
SyncE Clock Source Selection Mode: Auto
SyncE Active Clock Source Locked: No

SyncE Clock Source Status:
Port          Priority   Active Clock Source  Clock Status
-----
Eth 1/12      25        Yes                  Bad
...

```

**sync e force-clock-source-selecting** This command sets the local clock as the active clock source, or sets a port to be the active clock source.

### Syntax

**sync e force-clock-source-selecting** [**ethernet** *unit/port*]

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ If this command is used without specifying a clock source port, and SyncE has not been enabled on any port, then the local clock is set to be the active clock source.

- ◆ If SyncE has been enabled on more than one port, the switch will choose the clock source port based on the current clock source port status and priority.
- ◆ A port can be forced to be the clock source port regardless of the clock's signal status.

### Example

```
Console(config)#sync ethernet 1/12 clock-source priority 1  
Console(config)#
```

**sync ssm ethernet** This command configures a port to receive/send Synchronization Status Messages (SSM), and sets the priority used for this port in clock source port selection. Use the **no** form to stop using clock selection based on SSM.

### Syntax

**sync ssm ethernet** *unit/port* [**priority** *priority*]

**no sync ssm** [**ethernet** *unit/port*]

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*priority* - The priority used for clock source selection.  
(Range: 1-65535)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

#### General Information

- ◆ SSM provides a mechanism for downstream SyncE devices to synchronize with the Primary Reference Clock or the highest quality clock available. If an upstream network failure breaks this link, the synchronization function can take appropriate action based on SSM and pre-set priorities to select an alternate source of synchronization.
- ◆ This command only enables a port to send/receive SSM. It does not designate a specific port to be used as the clock source port. Use the [sync clk-src-ssm](#) command to configure the clock source.
- ◆ Only SSM will be extracted from the Ethernet Synchronization Message Channel (ESMC). No other information from the ESMC will be forwarded. SSM will be sent out of the specified port indicating the clock source selected by SSM or the manually configured clock source.

- ◆ The clock source port will not itself send out SSM. The other SSM-enabled ports will only send out SSM if received on the clock source port. SSM will be sent out of the other SSM-enabled ports once a second. If SSM has not been received on the clock source port after five seconds, the other SSM-enabled ports will stop sending SSM until a new clock source is selected.
- ◆ If SSM is disabled for a port, the priority level will be restored to the default value.

#### *Mode Changes*

- ◆ The switch can only be configured to use SSM for dynamic clock source selection when the current selection mode is set to Manual. The mode cannot be changed directly from SSM mode to Auto mode, or from Auto mode to SSM mode.
- ◆ If the switch is changed from SSM mode to Manual mode, and a port has been chosen as the active clock source in SSM mode, this port will still be the active clock source in Manual mode. If no clock source port has been selected in SSM mode, the local clock will be used as the active clock source.
- ◆ If the switch is changed from Manual mode to SSM mode, and a port has been chosen as the active clock source in Manual mode, this port will no longer be the active clock source. All clock source ports configured under Manual mode will be removed. The new active clock source is determined as described under the first item in this section.
- ◆ If the switch is changed from Manual mode to SSM mode using the **no** form of this command, and a port has been chosen as the active clock source in Auto mode, this port will be the active clock source in Manual Mode. If there is no active clock source in Auto mode, the local clock will be used as clock source in Manual mode. All ports configured as clock source ports under Auto mode will be kept after changing to Manual mode.

#### *Link State Changes*

- ◆ If an SSM-enabled port links up, the new active clock source is determined as described under the first item in this section.
- ◆ If SSM-chose clock source port goes down, the switch will choose the next clock source port as described under the first item in this section. If no other port can be used as the clock source port, the local clock will be used as the active clock source.

#### *Joining a Trunk*

- ◆ If an SSM-enabled port is added to a trunk, and the trunk is not operating at 1Gbps (full duplex), this port will no longer process SSM, and cannot be used a clock source port.

### Example

```
Console(config)#synce ssm ethernet 1/9
Console(config)#synce ssm ethernet 1/10
Console(config)#synce ssm ethernet 1/11
Console(config)#synce ssm ethernet 1/12
Console(config)#
```

**synce clk-src-ssm** This command uses SSM to select the clock source according to the SSM quality level, priority and port number. Use the no form to disable this function.

### Syntax

[no] **synce clk-src-ssm**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ Use this command to configure the clock source according to the SSM Quality Level (QL), port priority (as defined under the [synce ssm ethernet](#) command), and port number.

If the SSM QL received on more than one port is the same, the clock source port is selected according to priority.

If SSM QL and priority are the same on more than one port, the lower port number be chosen as the clock source port.

- ◆ If the clock source port has been manually configured (i.e., the active clock source is locked), SSM clock source selection will not function.

### Example

```
Console(config)#synce ssm ethernet 1/ 9
Console(config)#synce ssm ethernet 1/10
Console(config)#synce ssm ethernet 1/11
Console(config)#synce ssm ethernet 1/12
Console(config)#
```

**show synce** This command shows SyncE status, selection mode, clock source status, and SSM status.

### Command Mode

Privileged Exec

### Example

```

Console#show sync
SyncE Status:
Port          Status      Clock Source
-----
Eth 1/ 9  Enabled  No
Eth 1/10  Enabled  No
Eth 1/11  Enabled  No
Eth 1/12  Enabled  No
SyncE Clock Source Selection Mode: SSM
SyncE Active Clock Source Locked: No

SyncE Clock Source Status:
Port          Priority  Active Clock Source  Clock Status
-----
Eth 1/ 7          1          Yes                Good
Eth 1/ 8          2          No                 Bad

SyncE SSM Status:
Port          Status    Pri Tx SSM  Rx SSM
-----
Eth 1/ 9  Enabled    0 QL_NONE QL_EEC1
Eth 1/10  Enabled    0 QL-DNU  QL_EEC1
Eth 1/11  Enabled    0 QL_NONE QL_NONE
Eth 1/12  Enabled    0 QL_NONE QL_NONE
Console

```

**Table 27: show sync - display description for sync**

| Field                             | Description   |
|-----------------------------------|---|
| <b>SyncE Status</b>               |   |
| Port                              | Port identifier   |
| Status                            | Shows if SyncE is enabled or disabled   |
| Clock Source                      | Shows if port is configured as a clock source candidate   |
| SyncE Clock Source Selection Mode | Shows the clock source selection method: <ul style="list-style-type: none"> <li>♦ Manual – Manual mode (see <a href="#">sync</a> or <a href="#">sync ethernet</a> command)</li> <li>♦ Auto – Automatic mode (see <a href="#">sync auto-clock-source-selecting</a> command)</li> <li>♦ SSM – Selection based on SSM messages (see <a href="#">sync clk-src-ssm</a> command)</li> </ul> |
| SyncE Active Clock Source Locked  | Shows if clock source port is unlocked, or locked by manual or forced mode configuration  |
| <b>SyncE Clock Source Status</b>  |   |
| Port                              | Port identifier   |
| Priority                          | The selection priority determined by the manual configuration or default setting  |
| Active Clock Source               | Shows if port is currently operating as the port actively connected to the clock source   |
| Clock Status                      | Shows if the clock signal is valid or not   |
| <b>SyncE SSM Status</b>           |   |

**Table 27: show sync - display description for sync** (Continued)

| Field    | Description   |
|----------|---|
| Port     | Port identifier   |
| Status   | Shows if reception/transmission of SSM is enabled or disabled   |
| Priority | The selection priority determined by the manual configuration or default setting  |
| Tx SSM   | Shows transmitted Quality Level message type: <ul style="list-style-type: none"> <li>◆ QL-NONE: This port is not transmitting SSM or timeout information</li> <li>◆ QL-EEC1: Transmitting QL-EEC1* messages</li> <li>◆ QL-EEC2: Transmitting QL-EEC2* messages</li> </ul>   |
| Rx SSM   | Shows received Quality Level message type: <ul style="list-style-type: none"> <li>◆ QL-NONE: This port is not receiving SSM or timeout information</li> <li>◆ QL-DNU: This port is receiving SSM code but has not been chosen as the clock source port</li> <li>◆ QL-EEC1: Receiving QL-EEC1* messages</li> <li>◆ QL-EEC2: Receiving QL-EEC2* messages</li> </ul> |

\* The performance characteristics of the Phase Lock Loops (PLL) used to receive and re-transmit frequency synchronization signals in a SyncE chain are governed the ITU-T G.8262 standard. It defines two possible PLL performance options: Ethernet Equipment Clock (EEC) Option 1 and 2. EEC Option 1 is based on the 2.048 kbps hierarchy governed by G.813 Option 1 which is used in Europe and Asia. EEC Option 2 is based on the 1.544 kbps hierarchy governed by G.812 Type IV or Stratum 3 which is predominantly used in North America.

## 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 28: Switch Cluster Commands**

| Command                              | Function   | Mode |
|--------------------------------------|--|------|
| <code>cluster</code>                 | Configures clustering on the switch                | GC   |
| <code>cluster commander</code>       | Configures the switch as a cluster Commander       | GC   |
| <code>cluster ip-pool</code>         | Sets the cluster IP address pool for Members       | GC   |
| <code>cluster member</code>          | Sets Candidate switches as cluster members         | GC   |
| <code>rcommand</code>                | Provides configuration access to Member switches   | GC   |
| <code>show cluster</code>            | Displays the switch clustering status              | PE   |
| <code>show cluster members</code>    | Displays current cluster Members                   | PE   |
| <code>show cluster candidates</code> | Displays current cluster Candidates in the network | PE   |

### 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 527](#)).
  2. Add the participating ports to this VLAN (see [“Configuring VLAN Interfaces” on page 529](#)), 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 id** 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 ECS4810-12M is opened.
To end the CLI session, enter [Exit].

Vty-0#
```

**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  : ECS4810-12M
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  ECS4810-12M
CANDIDATE      00-12-CF-0B-47-A0  ECS4810-12M
Console#
```



# SNMP Commands

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 29: SNMP Commands**

| Command   | Function  | Mode   |
|---|---|--------|
| <i>General SNMP Commands</i>                                |   |        |
| <code>snmp-server</code>                                    | Enables the SNMP agent  | GC     |
| <code>snmp-server community</code>                          | Sets up the community access string to permit access to SNMP commands   | GC     |
| <code>snmp-server contact</code>                            | Sets the system contact string  | GC     |
| <code>snmp-server location</code>                           | Sets the system location string   | GC     |
| <code>show snmp</code>                                      | Displays the status of SNMP communications  | NE, PE |
| <i>SNMP Target Host Commands</i>                            |   |        |
| <code>snmp-server enable traps</code>                       | Enables the device to send SNMP traps (i.e., SNMP notifications)  | GC     |
| <code>snmp-server host</code>                               | Specifies the recipient of an SNMP notification operation   | GC     |
| <code>snmp-server enable port-traps mac-notification</code> | Enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed | IC     |
| <code>show snmp-server enable port-traps</code>             | Shows if SNMP traps are enabled or disabled for the specified interfaces  | PE     |
| <i>SNMPv3 Engine Commands</i>                               |   |        |
| <code>snmp-server engine-id</code>                          | Sets the SNMP engine ID   | GC     |
| <code>snmp-server group</code>                              | Adds an SNMP group, mapping users to views  | GC     |
| <code>snmp-server user</code>                               | Adds a user to an SNMP group  | GC     |
| <code>snmp-server view</code>                               | Adds an SNMP view   | GC     |
| <code>show snmp engine-id</code>                            | Shows the SNMP engine ID  | PE     |
| <code>show snmp group</code>                                | Shows the SNMP groups   | PE     |

**Table 29: SNMP Commands** (Continued)

| Command  | Function   | Mode      |
|--|--|-----------|
| <code>show snmp user</code>  | Shows the SNMP users   | PE        |
| <code>show snmp view</code>  | Shows the SNMP views   | PE        |
| <i>Notification Log Commands</i>   |  |           |
| <code>nlm</code>   | Enables the specified notification log   | GC        |
| <code>snmp-server notify-filter</code>                                   | Creates a notification log and specifies the target host   | GC        |
| <code>show nlm oper-status</code>  | Shows operation status of configured notification logs   | PE        |
| <code>show snmp notify-filter</code>                                     | Displays the configured notification logs  | PE        |
| <i>ATC Trap Commands</i>   |  |           |
| <code>snmp-server enable port-traps atc broadcast-alarm-clear</code>     | Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered  | IC (Port) |
| <code>snmp-server enable port-traps atc broadcast-alarm-fire</code>      | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control  | IC (Port) |
| <code>snmp-server enable port-traps atc broadcast-control-apply</code>   | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires  | IC (Port) |
| <code>snmp-server enable port-traps atc broadcast-control-release</code> | 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) |
| <code>snmp-server enable port-traps atc multicast-alarm-clear</code>     | Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered  | IC (Port) |
| <code>snmp-server enable port-traps atc multicast-alarm-fire</code>      | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control  | IC (Port) |
| <code>snmp-server enable port-traps atc multicast-control-apply</code>   | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires  | IC (Port) |
| <code>snmp-server enable port-traps atc multicast-control-release</code> | 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) |
| <i>Connectivity Fault Management Trap Commands</i>                       |  |           |
| <code>snmp-server enable traps ethernet cfm cc</code>                    | Enables SNMP traps for CFM continuity check events   | GC        |
| <code>snmp-server enable traps ethernet cfm crosscheck</code>            | Enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages | GC        |
| <i>Transceiver Power Threshold Trap Commands</i>                         |  |           |
| <code>transceiver-threshold current</code>                               | Sends a trap when the transceiver current falls outside the specified thresholds   | IC (Port) |
| <code>transceiver-threshold rx-power</code>                              | Sends a trap when the power level of the received signal falls outside the specified thresholds  | IC (Port) |
| <code>transceiver-threshold temperature</code>                           | Sends a trap when the transceiver temperature falls outside the specified thresholds   | IC (Port) |

**Table 29: SNMP Commands** (Continued)

| Command                                     | Function   | Mode      |
|---|--|-----------|
| <code>transceiver-threshold tx-power</code> | Sends a trap when the power level of the transmitted signal power outside the specified thresholds | IC (Port) |
| <code>transceiver-threshold voltage</code>  | Sends a trap when the transceiver voltage falls outside the specified thresholds                   | IC (Port) |
| <i>Additional Trap Commands</i>             |  |           |
| <code>memory</code>                         | Sets the rising and falling threshold for the memory utilization alarm                             | GC        |
| <code>process cpu</code>                    | Sets the rising and falling threshold for the CPU utilization alarm                                | GC        |
| <code>process cpu guard</code>              | Sets the CPU utilization watermark and threshold   | GC        |
| <code>show memory</code>                    | Shows memory utilization parameters  | PE        |
| <code>show process cpu</code>               | Shows CPU utilization parameters   | PE        |
| <code>show process cpu guard</code>         | Shows the CPU utilization watermark and threshold  | PE        |

## 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

**[no] snmp-server**

### Default Setting

Enabled

### Command Mode

Global Configuration

### Example

```
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

**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.

### 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 \(179\)](#)

**snmp-server location** This command sets the system location string. Use the **no** form to remove the location string.

### Syntax

**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

```
Console(config)#snmp-server location WC-19
Console(config)#
```

### Related Commands

[snmp-server contact \(178\)](#)

**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 | ethernet cfm | link-up-down | mac-notification [interval seconds]]**

**authentication** - Keyword to issue authentication failure notifications.

**ethernet cfm** - Connectivity Fault Management traps. For more information on these traps, see [“CFM Commands” on page 735](#).

**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 \(182\)](#)

**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 (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)

*retries* - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

*seconds* - 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 *Web Management Guide*.

*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 177](#)).
2. Create a view with the required notification messages ([page 189](#)).
3. Create a group that includes the required notify view ([page 186](#)).
4. Allow the switch to send SNMP traps; i.e., notifications ([page 180](#)).
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 177](#)).
  2. Create a remote SNMPv3 user to use in the message exchange process ([page 187](#)).
  3. Create a view with the required notification messages ([page 189](#)).
  4. Create a group that includes the required notify view ([page 186](#)).
  5. Allow the switch to send SNMP traps; i.e., notifications ([page 180](#)).
  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 \(180\)](#)

#### **snmp-server enable port-traps mac-notification**

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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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 or IPv6 address of the remote device.

*engineid-string* - String identifying the engine ID. (Range: 1-64 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 187).

### Example

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engine-id remote 9876543210 192.168.1.19
Console(config)#
```

### Related Commands

[snmp-server host \(182\)](#)

**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

```
snmp-server group groupname
{v1 | v2c | v3 {auth | noauth | priv}}
[read readview] [write writeview] [notify notifyview]
```

```
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 *Web Management 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<sup>1</sup> (read only), private<sup>2</sup> (read/write)

*readview* - Every object belonging to the Internet OID space (1).

*writeview* - Nothing is defined.

*notifyview* - Nothing is defined.

---

1. No view 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.
- ◆ For additional information on the notification messages supported by this switch, see the table for “Supported Notification Messages” in the *Web Management 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.

2. Maps to the defaultview.

**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 group 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 1.3.6.1.2.1.2.2.1.1.* 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 EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP Engine ID                               IP address
80000000030004e2b316c54321                          192.168.1.19
Console#
```

**Table 30: show snmp engine-id - display description**

| Field                  | Description   |
|------------------------|---|
| Local SNMP engineID    | String identifying the engine ID.   |
| Local SNMP engineBoots | The number of times that the engine has (re-)initialized since the snmp EngineID was last configured. |
| Remote SNMP engineID   | String identifying an engine ID on a remote device.   |
| IP address             | IP address of the device containing the corresponding remote SNMP engine.                             |

**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

Console#

```

**Table 31: show snmp group - display description**

| Field          | Description               |
|----------------|---------------------------|
| Group Name     | Name of an SNMP group.    |
| Security Model | The SNMP version.         |
| Read View      | The associated read view. |

**Table 31: show snmp group - display description** (Continued)

| Field        | Description                      |
|--------------|----------------------------------|
| Write View   | The associated write view.       |
| Notify View  | The associated notify view.      |
| Storage Type | The storage type for this entry. |
| Row Status   | The row status of this entry.    |

**show snmp user** This command shows information on SNMP users.

**Command Mode**  
Privileged Exec

### Example

```

Console#show snmp user
Engine ID           : 800001030300e00c0000fd0000
User Name           : steve
Group Name          : rd
Security Model      : v1
Security Level      : Authentication and privacy
Authentication Protocol : None
Privacy Protocol    : None
Storage Type        : Nonvolatile
Row Status          : Active

SNMP remote user
Engine ID           : 0000937564846450000
User Name           : mark
Group Name          : public
Security Model      : v3
Security Level      : Authentication and privacy
Authentication Protocol : MD5
Privacy Protocol    : DES56
Storage Type        : Nonvolatile
Row Status          : Active

Console#

```

**Table 32: show snmp user - display description**

| Field                   | Description   |
|-------------------------|---|
| Engine ID               | String identifying the engine ID.                   |
| User Name               | Name of user connecting to the SNMP agent.          |
| Group Name              | Name of an SNMP group.                              |
| Security Model          | The user security model: SNMP v1, v2c or v3.        |
| Security Level          | Indicates if authentication or encryption are used. |
| Authentication Protocol | The authentication protocol used with SNMPv3.       |
| Privacy Protocol        | The privacy protocol used with SNMPv3.              |

**Table 32: show snmp user - display description** (Continued)

| Field            | Description   |
|------------------|---|
| Storage Type     | The storage type for this entry.                          |
| Row Status       | The row status of this entry.                             |
| SNMP remote user | A user associated with an SNMP engine on a remote device. |

**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 33: show snmp view - display description**

| Field        | Description                                    |
|--------------|--|
| View Name    | Name of an SNMP view.                          |
| Subtree OID  | A branch in the MIB tree.                      |
| View Type    | Indicates if the view is included or excluded. |
| Storage Type | The storage type for this entry.               |
| Row Status   | The row status of this entry.                  |

## 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

None

### 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: 1-32 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.

```
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

```
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: 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(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

### Related Commands

[show memory \(104\)](#)

**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(config)#process cpu rising 80
Console(config)#process cpu falling 60
Console#
```

### Related Commands

[show process cpu \(104\)](#)

**process cpu guard** This command sets the CPU utilization high and low watermarks in percentage of CPU time utilized and the CPU high and low thresholds in the number of packets being processed per second. Use the **no** form of this command without any parameters to restore all of the default settings, or with a specific parameter to restore the default setting for that item.

### Syntax

**process cpu guard** [**high-watermark** *high-watermark* |  
**low-watermark** *low-watermark* | **max-threshold** *max-threshold* |  
**min-threshold** *min-threshold* | **trap**]

*high-watermark* - If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark.

*low-watermark* - If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark.

*max-threshold* - If the number of packets being processed per second by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold.

*min-threshold* - If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold.

**trap** - If traps are enabled, the switch will send an alarm message if CPU utilization exceeds the high watermark in percentage of CPU usage time or exceeds the maximum threshold in the number of packets being processed by the CPU.

### Default Setting

Guard Status: Disabled  
High Watermark: 90%  
Low Watermark: 70%  
Maximum Threshold: 500 packets per second  
Minimum Threshold: 50 packets per second  
Trap Status: Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ Once the high watermark is exceeded, utilization must drop beneath the low watermark before the alarm is terminated, and then exceed the high watermark again before another alarm is triggered.

- ◆ Once the maximum threshold is exceeded, utilization must drop beneath the minimum threshold before the alarm is terminated, and then exceed the maximum threshold again before another alarm is triggered.

### Example

```
Console(config)#process cpu guard high-watermark 80  
Console(config)#process cpu guard low-watermark 60  
Console(config)#
```

### Related Commands

[show process cpu guard \(105\)](#)



# 6

## Remote Monitoring Commands

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 34: RMON Commands**

| Command                              | Function                                       | Mode |
|--------------------------------------|--|------|
| <code>rmon alarm</code>              | Sets threshold bounds for a monitored variable | GC   |
| <code>rmon event</code>              | Creates a response event for an alarm          | GC   |
| <code>rmon collection history</code> | Periodically samples statistics                | IC   |
| <code>rmon collection rmon1</code>   | Enables statistics collection                  | IC   |
| <code>show rmon alarms</code>        | Shows the settings for all configured alarms   | PE   |
| <code>show rmon events</code>        | Shows the settings for all configured events   | PE   |
| <code>show rmon history</code>       | Shows the sampling parameters for each entry   | PE   |
| <code>show rmon statistics</code>    | Shows the collected statistics                 | PE   |

**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: 1-65535)

*name* – Name of the person who created this entry. (Range: 1-127 characters)

### Default Setting

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.12  
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

```
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
Console(config)#
```

**rmon event** This command creates a response event for an alarm. Use the **no** form to remove an event.

### Syntax

**rmon event** *index* [**log**] | [**trap** *community*] | [**description** *string*] | [**owner** *name*]

**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 136](#)).

**trap** – Sends a trap message to all configured trap managers (see the [snmp-server host](#) command).

*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: 1-32 characters)

*string* – A comment that describes this event. (Range: 1-127 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*

*index* – Index to this entry. (Range: 1-65535)

*number* – The number of buckets requested for this entry. (Range: 1-65536)

*seconds* – The polling interval. (Range: 1-3600 seconds)

*name* – Name of the person who created this entry.  
 (Range: 1-127 characters)

**Default Setting**

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.12

Buckets: 50

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 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
Console(config-if)#
```

**rmon collection rmon1** This command enables the collection of statistics on a physical interface. Use the `rmon1` 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: 1-127 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 controentry 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#show rmon history
Entry 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 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#show rmon statistics
Interface 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 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
:

```



## 7

# Flow Sampling Commands

Flow sampling (sFlow) can be used with a remote sFlow Collector to provide an accurate, detailed and real-time overview of the types and levels of traffic present on the network. The sFlow Agent samples 1 out of  $n$  packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place.



**Note:** The terms “collector”, “receiver” and “owner”, in the context of this chapter, all refer to a remote server capable of receiving the sFlow datagrams generated by the sFlow agent of the switch.

**Table 35: sFlow Commands**

| Command                              | Function  | Mode |
|--------------------------------------|---|------|
| <code>sflow owner</code>             | Creates an sFlow collector which the switch uses to send samples to.                        | PE   |
| <code>sflow polling instance</code>  | Configures an sFlow polling data source that takes samples periodically based on time.      | PE   |
| <code>sflow sampling instance</code> | Configures an sFlow sampling data source that samples periodically based on a packet count. | PE   |
| <code>show sflow</code>              | Shows the global and interface settings for the sFlow process                               | PE   |

**sflow owner** This command creates an sFlow collector on the switch. Use the **no** form to remove the sFlow receiver.

## Syntax

```
sflow owner owner-name
timeout timeout-value
[destination {ipv4-address | ipv6-address}] [port destination-udp-port]
[max-datagram-size max-datagram-size]
[version {v4 | v5}]
```

```
no sflow owner owner-name
```

*owner-name* - Name of the collector. (Range: 1-30 alphanumeric characters)

*timeout-value* - The length of time the sFlow interface is available to send samples to a receiver, after which the owner and associated polling and sampling data source instances are removed from the configuration. (Range: 30-10000000 seconds)

*ipv4-address* - IPv4 address of the sFlow collector. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods.

*ipv6-address* - IPv6 address of the sFlow collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 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.

*destination-udp-port* - The UDP port on which the collector is listening for sFlow streams. (Range: 1-65535)

*max-datagram-size* - The maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)

**version {v4 | v5}** - Sends either v4 or v5 sFlow datagrams to the receiver.

### Default Setting

No owner is configured

UDP Port: 6343

Version: v4

Maximum Datagram Size: 1400 bytes

### Command Mode

Privileged Exec

### Command Usage

- ◆ Use the **sflow owner** command to create an owner instance of an sFlow collector. If the socket port, maximum datagram size, and datagram version are not specified, then the default values are used.
- ◆ Once an owner is created, the **sflow owner** command can again be used to modify the owner's port number. All other parameter values for the owner will be retained if the port is modified.
- ◆ Use the **no sflow owner** command to remove the collector.
- ◆ When the **sflow owner** command is issued, its associated timeout value will immediately begin to count down. Once the timeout value has reached zero seconds, the sFlow owner and its associated sampling sources will be deleted from the configuration.

### Example

This example shows an sflow collector being created on the switch.

```

Console(config)#sflow owner stat_server1 timeout 100 destination
192.168.220.225 port 22500 max-datagram-size 512 version v5
Console(config)#

```

This example shows how to modify the sFlow port number for an already configured collector.

```

Console(config)#sflow owner stat_server1 timeout 100 port 35100
Console(config)#

```

**sflow polling instance** This command enables an sFlow polling data source, for a specified interface, that polls periodically based on a specified time interval. Use the **no** form to remove the polling data source instance from the switch's sFlow configuration.

### Syntax

**sflow polling** {**interface** *interface*} **instance** *instance-id* **receiver** *owner-name*  
**polling-interval** *seconds*

**no sflow polling** {**interface** *interface*} **instance** *instance-id*

*interface* - The source from which the samples will be taken at specified intervals and sent to a collector.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*instance-id* - An instance ID used to identify the sampling source. (Range: 1)

*owner-name* - The associated receiver, to which the samples will be sent. (Range: 1-30 alphanumeric characters)

**polling-interval** - The time interval at which the sFlow process adds counter values to the sample datagram. (Range: 0-10000000 seconds, 0 disables this feature)

### Default Setting

No sFlow polling instance is configured.

### Command Mode

Privileged Exec

### Command Usage

This command enables a polling data source and configures the interval at which counter values are added to the sample datagram.

**Example**

This example sets the polling interval to 10 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow polling-interval 10
Console(config-if)#
```

**sflow sampling instance** This command enables an sFlow data source instance for a specific interface that takes samples periodically based on the number of packets processed. Use the **no** form to remove the sampling data source instance from the switch's sFlow configuration.

**Syntax**

**sflow sampling** {**interface** *interface*} **instance** *instance-id* **receiver** *owner-name*  
**sampling-rate** *sample-rate*  
 [**max-header-size** *max-header-size*]

**no sflow sample** {**interface** *interface*} **instance** *instance-id*

*interface* - The source from which the samples will be taken and sent to a collector.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*instance-id* - An instance ID used to identify the sampling source. (Range: 1)

*owner-name* - The associated receiver, to which the samples will be sent. (Range: 1-30 alphanumeric characters)

*sample-rate* - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 256-16777215 packets)

*max-header-size* - The maximum size of the sFlow datagram header. (Range: 64-256 bytes)

**Default Setting**

No sFlow sampling instance id configured.

Maximum Header Size: 128 bytes

**Command Mode**

Privileged Exec

**Example**

This example enables a sampling data source on Ethernet interface 1/1, an associated receiver named "owner1", and a sampling rate of one out of 100. The maximum header size is also set to 200 bytes.

```
Console# sflow sampling interface ethernet 1/1 instance 1 receiver owner1
sampling-rate 100 max-header-size 200
Console#
```

The following command removes a sampling data source from Ethernet interface 1/1.

```
Console# no sflow sampling interface ethernet 1/1 instance 1
Console#
```

**show sflow** This command shows the global and interface settings for the sFlow process.

**Syntax**

**show sflow** [**owner** *owner-name* | **interface** *interface*]

*owner-name* - The associated receiver, to which the samples are sent.  
(Range: 1-30 alphanumeric characters)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**Command Mode**

Privileged Exec

**Example**

```
Console#show sflow interface ethernet 1/2

Receiver Owner Name      : stat1
Receiver Timeout         : 99633 sec
Receiver Destination     : 192.168.32.32
Receiver Socket Port     : 6343
Maximum Datagram Size    : 1400 bytes
Datagram Version         : 4

Data Source               : Eth 1/2
Sampling Instance ID     : 1
Sampling Rate             : 512
Maximum Header Size      : 128 bytes

Console#
```



# 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<sup>3</sup> to the data ports.

**Table 36: Authentication Commands**

| Command Group                              | Function  |
|--|---|
| <a href="#">User Accounts</a>              | Configures the basic user names and passwords for management access   |
| <a href="#">Authentication Sequence</a>    | Defines logon authentication method and precedence  |
| <a href="#">RADIUS Client</a>              | Configures settings for authentication via a RADIUS server  |
| <a href="#">TACACS+ Client</a>             | Configures settings for authentication via a TACACS+ server   |
| <a href="#">AAA</a>                        | Configures authentication, authorization, and accounting for network access   |
| <a href="#">Web Server</a>                 | Enables management access via a web browser   |
| <a href="#">Telnet Server</a>              | Enables management access via Telnet  |
| <a href="#">Secure Shell</a>               | Provides secure replacement for Telnet  |
| <a href="#">802.1X Port Authentication</a> | Configures host authentication on specific ports using 802.1X   |
| <a href="#">Management IP Filter</a>       | Configures IP addresses that are allowed management access  |
| <a href="#">PPPoE Intermediate Agent</a>   | Configures relay parameters required for sending authentication messages between a client and broadband remote access servers |

3. For other methods of controlling client access, see [“General Security Measures” on page 279](#).

## User Accounts

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 125), user authentication via a remote authentication server (page 215), and host access authentication for specific ports (page 252).

Table 37: User Access Commands

| Command                      | Function   | Mode |
|------------------------------|--|------|
| <code>enable password</code> | Sets a password to control access to the Privileged Exec level | GC   |
| <code>username</code>        | Establishes a user name-based authentication system at login   | GC   |

**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** - Level 15 for Privileged Exec. (Levels 0-14 are not used.)

{**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 admin
Console(config)#
```

### Related Commands

[enable \(85\)](#)

[authentication enable \(218\)](#)

**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* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}

**no username** *name*

*name* - The name of the user. (Maximum length: 8 characters, case sensitive. Maximum users: 16)

**access-level** *level* - Specifies the user level.

The device has two predefined privilege levels:

**0**: Normal Exec, **15**: Privileged Exec.

**nopassword** - No password is required for this user to log in.

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

**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 38: Default Login Settings**

| username | access-level | password |
|----------|--------------|----------|
| guest    | 0            | guest    |
| admin    | 15           | admin    |

### 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)#
```

## 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 39: Authentication Sequence Commands

| Command                            | Function   | Mode |
|------------------------------------|--|------|
| <code>authentication enable</code> | Defines the authentication method and precedence for command mode change | GC   |
| <code>authentication login</code>  | Defines logon authentication method and precedence                       | GC   |

**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(config)#authentication enable radius  
Console(config)#
```

### Related Commands

[enable password](#) - sets the password for changing command modes (216)

**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**

**local** - Use local password.

**radius** - Use RADIUS server password.

**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 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  
Console(config)#
```

### Related Commands

[username](#) - for setting the local user names and passwords (217)

---

## 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 40: RADIUS Client Commands

| Command                                  | Function  | Mode |
|--|---|------|
| <a href="#">radius-server acct-port</a>  | Sets the RADIUS server network port                       | GC   |
| <a href="#">radius-server auth-port</a>  | Sets the RADIUS server network port                       | GC   |
| <a href="#">radius-server host</a>       | Specifies the RADIUS server                               | GC   |
| <a href="#">radius-server key</a>        | Sets the RADIUS encryption key                            | GC   |
| <a href="#">radius-server retransmit</a> | Sets the number of retries                                | GC   |
| <a href="#">radius-server timeout</a>    | Sets the interval between sending authentication requests | GC   |
| <a href="#">show radius-server</a>       | Shows the current RADIUS settings                         | PE   |

**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)

**Default Setting**

1813

**Command Mode**

Global Configuration

**Example**

```
Console(config)#radius-server acct-port 181
Console(config)#
```

**radius-server acct-port** This command sets the RADIUS server network port. 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 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. Do not use blank spaces in the string. (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 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* - 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#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 41: TACACS+ Client Commands**

| Command                                  | Function  | Mode |
|--|---|------|
| <a href="#">tacacs-server host</a>       | Specifies the TACACS+ server and optional parameters      | GC   |
| <a href="#">tacacs-server key</a>        | Sets the TACACS+ encryption key                           | GC   |
| <a href="#">tacacs-server port</a>       | Specifies the TACACS+ server network port                 | GC   |
| <a href="#">tacacs-server retransmit</a> | Sets the number of retries                                | GC   |
| <a href="#">tacacs-server timeout</a>    | Sets the interval between sending authentication requests | GC   |
| <a href="#">show tacacs-server</a>       | Shows the current TACACS+ settings                        | GC   |

**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.  
Do not use blank spaces in the string.  
(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  : 10.11.12.13  
Server Port Number : 49  
Retransmit Times   : 2  
Timeout           : 4
```

```
TACACS+ Server Group:
Group Name          Member Index
-----
tacacs+             1
Console#
```

## AAA

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 42: AAA Commands**

| Command                             | Function  | Mode |
|-------------------------------------|---|------|
| <code>aaa accounting dot1x</code>   | Enables accounting of 802.1X services                                       | GC   |
| <code>aaa accounting exec</code>    | Enables accounting of Exec services   | GC   |
| <code>aaa accounting update</code>  | Enables periodoc updates to be sent to the accounting server                | GC   |
| <code>aaa authorization exec</code> | Enables authorization of Exec sessions                                      | GC   |
| <code>aaa group server</code>       | Groups security servers in to defined lists                                 | GC   |
| <code>server</code>                 | Configures the IP address of a server in a group list                       | SG   |
| <code>accounting dot1x</code>       | Applies an accounting method to an interface for 802.1X service requests    | IC   |
| <code>accounting exec</code>        | Applies an accounting method to local console, Telnet or SSH connections    | Line |
| <code>authorization exec</code>     | Applies an authorization method to local console, Telnet or SSH connections | Line |
| <code>show accounting</code>        | Displays all accounting information   | PE   |

**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: 1-64 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: 1-64 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 disable accounting updates.

### Syntax

**aaa accounting update** [*periodic interval*]

**no aaa accounting update**

*interval* - Sends an interim accounting record to the server at this interval.  
(Range: 1-2147483647 minutes)

### Default Setting

1 minute

### 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 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 for local console, Telnet, or SSH connections.
- ◆ 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: 1-64 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 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 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** [[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] | **exec** [**statistics**] | **statistics**]

*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: 1-12)

### 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+
  Interface     : vty
Console#
```

## Web Server

This section describes commands used to configure web browser management access to the switch.

**Table 43: Web Server Commands**

| Command                               | Function   | Mode |
|---------------------------------------|--|------|
| <a href="#">ip http port</a>          | Specifies the port to be used by the web browser interface     | GC   |
| <a href="#">ip http server</a>        | Allows the switch to be monitored or configured from a browser | GC   |
| <a href="#">ip http secure-port</a>   | Specifies the TCJP port number for HTTPS                       | GC   |
| <a href="#">ip http secure-server</a> | Enables HTTPS (HTTP/SSL) for encrypted communications          | GC   |



**Note:** Users are automatically logged off of the HTTP server or HTTPS server if no input is detected for 300 seconds.

**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 \(237\)](#)

[show system \(108\)](#)

**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
Console(config)#
```

#### Related Commands

[ip http port \(236\)](#)

[show system \(108\)](#)

**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, except for the following reserved ports: 1 and 25 - Linux kernel, 23 - Telnet, 80 - HTTP)

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

### Related Commands

[ip http secure-server \(238\)](#)

[show system \(108\)](#)

**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

**[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 11, Mozilla Firefox 40, or Google Chrome 45, or more recent versions.

The following web browsers and operating systems currently support HTTPS:

**Table 44: HTTPS System Support**

| Web Browser                   | Operating System        |
|-------------------------------|-------------------------|
| Internet Explorer 11 or later | Windows 7, 8, 10        |
| Mozilla Firefox 40 or later   | Windows 7, 8, 10, Linux |
| Google Chrome 45 or later     | Windows 7, 8, 10        |

- ◆ To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” in the *Web Management 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 \(237\)](#)
- [copy tftp https-certificate \(115\)](#)
- [show system \(108\)](#)

## Telnet Server

This section describes commands used to configure Telnet management access to the switch.

**Table 45: Telnet Server Commands**

| Command                                | Function   | Mode |
|--|--|------|
| <a href="#">ip telnet max-sessions</a> | Specifies the maximum number of Telnet sessions that can simultaneously connect to this system | GC   |
| <a href="#">ip telnet port</a>         | Specifies the port to be used by the Telnet interface  | GC   |
| <a href="#">ip telnet server</a>       | Allows the switch to be monitored or configured from Telnet                                    | GC   |
| <a href="#">telnet (client)</a>        | Accesses a remote device using a Telnet connection   | PE   |
| <a href="#">show ip telnet</a>         | Displays configuration settings for the Telnet server  | PE   |



**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 eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number of eight 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)#
```

**telnet (client)** This command accesses a remote device using a Telnet connection.

### Syntax

**telnet** *host*

*host* - IP address or alias of a remote device.

### Command Mode

Privileged Exec

### Example

```
Console#telnet 192.168.2.254  
Connect To 192.168.2.254...  
  
*****  
  
WARNING - MONITORED ACTIONS AND ACCESSES  
  
User Access Verification  
  
Username:  
  
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: 4
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.

**Table 46: Secure Shell Commands**

| Command                                      | Function   | Mode |
|--|--|------|
| <code>ip ssh authentication-retries</code>   | Specifies the number of retries allowed by a client  | GC   |
| <code>ip ssh server</code>                   | Enables the SSH server on the switch   | GC   |
| <code>ip ssh server-key size</code>          | Sets the SSH server key size   | GC   |
| <code>ip ssh timeout</code>                  | Specifies the authentication timeout for the SSH server  | GC   |
| <code>copy tftp public-key</code>            | Copies the user's public key from a TFTP server to the switch  | PE   |
| <code>delete public-key</code>               | Deletes the public key for the specified user  | PE   |
| <code>disconnect</code>                      | Terminates a line connection   | PE   |
| <code>ip ssh crypto host-key generate</code> | Generates the host key   | PE   |
| <code>ip ssh crypto zeroize</code>           | Clear the host key from RAM  | PE   |
| <code>ip ssh save host-key</code>            | Saves the host key from RAM to flash memory  | PE   |
| <code>show ip ssh</code>                     | Displays the status of the SSH server and the configured values for authentication timeout and retries | PE   |
| <code>show public-key</code>                 | Shows the public key for the specified user or for the host  | PE   |

**Table 46: Secure Shell Commands** (Continued)

| Command                 | Function   | Mode |
|-------------------------|--|------|
| <code>show ssh</code>   | Displays the status of current SSH sessions                    | PE   |
| <code>show users</code> | Shows SSH users, including privilege level and public key type | PE   |

*Configuration Guidelines*

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:

```
10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
15020245593199868544358361651999923329781766065830956
108259132128902337654680172627257141342876294130119619556678259566410486957427
888146206519417467729848654686157177393901647793559423035774130980227370877945
4524083971752646358058176716709574804776117
```

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
134108168560989392104094492015542534763164192187295892114317388005553616163105
177594083868631109291232226828519254374603100937187721199696317813662774141689
851320491172048303392543241016379975923714490119380060902539484084827178194372
288402533115952134861022902978982721353267131629432532818915045306393916643
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)*

- a. The client sends its password to the server.
- b. The switch compares the client's password to those stored in memory.
- c. If a match is found, the connection is allowed.



**Note:** To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

*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*

- a. The client sends its RSA public key to the switch.
- b. 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(config)#ip ssh authentication-retries 2
Console(config)#
```

#### Related Commands

[show ip ssh \(250\)](#)

**ip ssh server** This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

#### Syntax

**[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#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

### Related Commands

[ip ssh crypto host-key generate \(248\)](#)  
[show ssh \(251\)](#)

**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: 512-896 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 \(127\)](#)

[show ip ssh \(250\)](#)

**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

```
Console#ip ssh crypto host-key generate dsa  
Console#
```

### Related Commands

[ip ssh crypto zeroize \(249\)](#)

[ip ssh save host-key \(249\)](#)

**ip ssh crypto zeroize** This command clears the host key from memory (i.e. RAM).

#### Syntax

**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

```
Console#ip ssh crypto zeroize dsa
Console#
```

#### Related Commands

[ip ssh crypto host-key generate \(248\)](#)

[ip ssh save host-key \(249\)](#)

[no ip ssh server \(245\)](#)

**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

[ip ssh crypto host-key generate \(248\)](#)

**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 13236940658254764031382795526536375927835525327972629521130241
071942106165575942459093923609695405036277525755625100386613098939383452310
332802149888661921595568598879891919505883940181387440468908779160305837768
```

```

185490002831341625008348718449522087429212255691665655296328163516964040831
5547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKx15fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PwxDZMacNBpjBrRAAAAFQChb4vsdfQGNIjwbv
wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnr fwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOFT/yyEfbobMJZi8oGCst.SNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq70+jAhf1Dg451oAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFACzWS7EjOy
Dbs1oBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAWecsigF/+DjKGWtPNIQgabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
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 47: show ssh - display description**

| Field      | Description   |
|------------|---|
| Connection | The session number. (Range: 0-3)  |
| Version    | The Secure Shell version number.  |
| State      | The authentication negotiation state.<br>(Values: Negotiation-Started, Authentication-Started, Session-Started) |
| Username   | The user name of the client.  |

## 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 48: 802.1X Port Authentication Commands**

| Command                                  | Function   | Mode |
|--|--|------|
| <i>General Commands</i>                  |  |      |
| <code>dot1x default</code>               | Resets all dot1x parameters to their default values  | GC   |
| <code>dot1x eapol-pass-through</code>    | Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled   | GC   |
| <code>dot1x system-auth-control</code>   | Enables dot1x globally on the switch.  | GC   |
| <i>Authenticator Commands</i>            |  |      |
| <code>dot1x intrusion-action</code>      | Sets the port response to intrusion when authentication fails  | IC   |
| <code>dot1x max-reauth-req</code>        | Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process          | IC   |
| <code>dot1x max-req</code>               | 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 | IC   |
| <code>dot1x operation-mode</code>        | Allows single or multiple hosts on an dot1x port   | IC   |
| <code>dot1x port-control</code>          | Sets dot1x mode for a port interface   | IC   |
| <code>dot1x re-authentication</code>     | Enables re-authentication for all ports  | IC   |
| <code>dot1x timeout quiet-period</code>  | Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client                           | IC   |
| <code>dot1x timeout re-authperiod</code> | Sets the time period after which a connected client must be re-authenticated   | IC   |
| <code>dot1x timeout supp-timeout</code>  | Sets the interval for a supplicant to respond  | IC   |
| <code>dot1x timeout tx-period</code>     | Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet   | IC   |
| <code>dot1x re-authenticate</code>       | Forces re-authentication on specific ports   | PE   |
| <i>Supplicant Commands</i>               |  |      |
| <code>dot1x identity profile</code>      | Configures dot1x supplicant user name and password   | GC   |
| <code>dot1x max-start</code>             | Sets the maximum number of times that a port supplicant will send an EAP start frame to the client   | IC   |
| <code>dot1x pae supplicant</code>        | Enables dot1x supplicant mode on an interface  | IC   |
| <code>dot1x timeout auth-period</code>   | Sets the time that a supplicant port waits for a response from the authenticator   | IC   |

**Table 48: 802.1X Port Authentication Commands** (Continued)

| Command                                 | Function   | Mode |
|---|--|------|
| <code>dot1x timeout held-period</code>  | Sets the time a port waits after the maximum start count has been exceeded before attempting to find another authenticator | IC   |
| <code>dot1x timeout start-period</code> | Sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator                      | IC   |
| <i>Information Display Commands</i>     |  |      |
| <code>show dot1x</code>                 | Shows all dot1x related information  | PE   |

## General Commands

**dot1x default** This command sets all configurable dot1x 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`
- ◆ `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)#
```

**dot1x eapol-pass-through** 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).
- ◆ A port can only be assigned to the guest VLAN in case of failed authentication, if [switchport mode](#) is set to Hybrid.

### 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 host 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 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(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

### Related Commands

[dot1x timeout re-authperiod \(259\)](#)

**dot1x timeout quiet-period** This command sets the time that a switch port waits after the maximum request count (see [page 256](#)) 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(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(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

**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(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

**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: 1-12)

### 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: 1-8 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 eth 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: 1-12)

### 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 254](#)).
- ◆ *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled ([page 254](#)).
- ◆ *Supplicant Parameters* – Shows the supplicant user name used when the switch responds to an MD5 challenge from an authenticator ([page 261](#)).
- ◆ *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 256](#)).
  - Control Mode – Dot1x port control mode ([page 257](#)).
  - Authorized – Authorized 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 258](#)).
  - Reauth Period – Time after which a connected client must be re-authenticated ([page 259](#)).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client ([page 258](#)).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet ([page 260](#)).

- 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 256).
- 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 257).
- Intrusion Action– Shows the port response to intrusion when authentication fails (page 255).
- Supplicant– MAC address of authorized client.

◆ *Authenticator PAE State Machine*

- State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force\_authorized, force\_unauthorized).
- 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**

```
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

Port      Type      Operation Mode Control Mode      Authorized
-----
Eth 1/ 1 Disabled  Single-Host      Force-Authorized  Yes
```

```
Eth 1/ 2 Disabled      Single-Host   Force-Authorized  Yes
.
.
Eth 1/11 Disabled     Single-Host   Force-Authorized  Yes
Eth 1/12 Enabled      Single-Host   Auto               Yes
```

802.1X Port Details

```
802.1X Authenticator is enabled on port 1/1
802.1X Supplicant is disabled on port 1/1
```

```
.
.
Console#show dot1x interface ethernet 1/10
```

```
802.1X Authenticator is enabled on port 10
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
```

```
Backend State Machine
State                : Idle
Request Count        : 0
Identifier(Server)   : 2
```

```
Reauthentication State Machine
State                : Initialize
```

```
Console#
```

---

## Management IP Filter

This section describes commands used to configure IP management access to the switch.

**Table 49: Management IP Filter Commands**

| Command                      | Function   | Mode |
|------------------------------|--|------|
| <code>management</code>      | Configures IP addresses that are allowed management access       | GC   |
| <code>show management</code> | Displays the switch to be monitored or configured from a browser | PE   |

**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.

*end-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#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 50: PPPoE Intermediate Agent Commands

| Command  | Function   | Mode |
|--|--|------|
| <code>pppoe intermediate-agent</code>                  | Enables the PPPoE IA globally on the switch  | GC   |
| <code>pppoe intermediate-agent format-type</code>      | Sets the access node identifier and generic error message for the switch                   | GC   |
| <code>pppoe intermediate-agent port-enable</code>      | Enables the PPPoE IA on an interface   | IC   |
| <code>pppoe intermediate-agent port-format-type</code> | Sets the circuit-id or remote-id for an interface  | IC   |
| <code>pppoe intermediate-agent trust</code>            | Sets the trust mode for an interface   | IC   |
| <code>pppoe intermediate-agent vendor-tag strip</code> | Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server | IC   |
| <code>clear pppoe intermediate-agent statistics</code> | Clears PPPoE IA statistics   | PE   |
| <code>show pppoe intermediate-agent info</code>        | Displays PPPoE IA configuration settings   | PE   |
| <code>show pppoe intermediate-agent statistics</code>  | Displays PPPoE IA statistics   | PE   |

**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 an 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 management interface.
- ◆ 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)#
```

**pppoe  
 intermediate-agent  
 port-format-type**

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).

**Example**

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id
ECS4500-28
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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**Command Mode**

Privileged Exec

**Example**

```
Console#show pppoe intermediate-agent info
PPPoE Intermediate Agent Global Status      : Disabled
PPPoE Intermediate Agent Admin Access Node Identifier :
```

```

PPPoE Intermediate Agent Oper Access Node Identifier : 192.168.2.14
PPPoE Intermediate Agent Admin Generic Error Message :
PPPoE Intermediate Agent Oper Generic Errnr Mdssage :
  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 1/1   No       No       No
                                         Oper Circuit-ID Oper Remote-ID  }
                                         -----
                                         1/1:vid         70-72-CF-59-8F-41

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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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

Console#
  
```

**Table 51: show pppoe intermediate-agent statistics - display description**

| Field           | Description                       |
|-----------------|-----------------------------------|
| <i>Received</i> |                                   |
| PADI            | PPPoE Active Discovery Initiation |

**Table 51: show pppoe intermediate-agent statistics - display description**  
 (Continued)

| Field                     | Description  |
|---------------------------|--|
| PADO                      | PPPoE Active Discovery Offer                                       |
| PADR                      | PPPoE Active Discovery Request                                     |
| PADS                      | PPPoE Active Discovery Session-Confirmation                        |
| PADT                      | PPPoE Active Discovery Terminate                                   |
| <i>Dropped</i>            |  |
| Response from untrusted   | Response from an interface which not been configured as trusted.   |
| Request towards untrusted | Request sent to an interface which not been configured as trusted. |
| Malformed                 | Corrupted PPPoE message.   |



# 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 52: General Security Commands**

| Command Group                   | Function  |
|---------------------------------|---|
| Port Security*                  | Configures secure addresses for a port  |
| 802.1X Port Authentication*     | Configures host authentication on specific ports using 802.1X   |
| Network Access*                 | Configures MAC authentication and dynamic VLAN assignment   |
| Web Authentication*             | Configures Web authentication   |
| Access Control Lists*           | 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) |
| DHCP Snooping*                  | Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table   |
| IP Source Guard*                | Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings                             |
| ARP Inspection                  | Validates the MAC-to-IP address bindings in ARP packets   |
| DoS Protection                  | Protects against Denial-of-Service attacks  |
| Port-based Traffic Segmentation | Configures traffic segmentation for different client sessions based on specified downlink and uplink ports  |

\* 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 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 53: Management IP Filter Commands**

| Command                               | Function   | Mode |
|---------------------------------------|--|------|
| <code>mac-address-table static</code> | Maps a static address to a port in a VLAN              | GC   |
| <code>port security</code>            | Configures a secure port                               | IC   |
| <code>show mac-address-table</code>   | Displays entries in the bridge-forwarding database     | PE   |
| <code>show port security</code>       | Displays port security status and secure address count | PE   |

**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 security violation or for the maximum number of allowed addresses.

### Syntax

**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 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, 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. 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 \(377\)](#)

[mac-address-table static \(454\)](#)

**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: 1-12)

### 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
Eth 1/ 6  Disabled      Secure/Down      None          0          0
Eth 1/ 7  Disabled      Secure/Down      None          0          0
Eth 1/ 8  Disabled      Secure/Down      None          0          0
Eth 1/ 9  Disabled      Secure/Down      None          0          0
Eth 1/10  Disabled      Secure/Down      None          0          0
Eth 1/11  Disabled      Secure/Down      None          0          0
Eth 1/12  Disabled      Secure/Down      None          0          0
Console#
```

**Table 54: show port security - display description**

| Field            | Description   |
|------------------|---|
| Port Security    | The configured status (enabled or disabled).  |
| Port Status      | The operational status: <ul style="list-style-type: none"> <li>◆ Secure/Down – Port security is disabled.</li> <li>◆ Secure/Up – Port security is enabled.</li> <li>◆ Shutdown – Port is shut down due to a response to a port security violation.</li> </ul> |
| Intrusion Action | The configured intrusion response.  |
| MaxMacCnt        | The maximum number of addresses which can be stored in the address table for this interface (either dynamic or static).   |
| CurrMacCnt       | The current number of secure entries in the address 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 : 2Disabled
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 55: Network Access Commands**

| Command   | Function   | Mode |
|---|--|------|
| <code>network-access aging</code>                       | Enables MAC address aging  | GC   |
| <code>network-access mac-filter</code>                  | Adds a MAC address to a filter table   | GC   |
| <code>mac-authentication reauth-time</code>             | Sets the time period after which a connected MAC address must be re-authenticated                            | GC   |
| <code>network-access dynamic-qos</code>                 | Enables the dynamic quality of service feature   | IC   |
| <code>network-access dynamic-vlan</code>                | Enables dynamic VLAN assignment from a RADIUS server   | IC   |
| <code>network-access guest-vlan</code>                  | Specifies the guest VLAN   | IC   |
| <code>network-access link-detection</code>              | Enables the link detection feature   | IC   |
| <code>network-access link-detection link-down</code>    | Configures the link detection feature to detect and act upon link-down events                                | IC   |
| <code>network-access link-detection link-up</code>      | Configures the link detection feature to detect and act upon link-up events                                  | IC   |
| <code>network-access link-detection link-up-down</code> | Configures the link detection feature to detect and act upon both link-up and link-down events               | IC   |
| <code>network-access max-mac-count</code>               | Sets the maximum number of MAC addresses that can be authenticated on a port via all forms of authentication | IC   |
| <code>network-access mode mac-authentication</code>     | Enables MAC authentication on an interface   | IC   |
| <code>network-access port-mac-filter</code>             | Enables the specified MAC address filter   | IC   |
| <code>mac-authentication intrusion-action</code>        | Determines the port response when a connected host fails MAC authentication.                                 | IC   |
| <code>mac-authentication max-mac-count</code>           | Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication          | IC   |
| <code>clear network-access mac-address-table</code>     | Clears authenticated MAC addresses from the address table  | PE   |
| <code>show network-access</code>                        | Displays the MAC authentication settings for port interfaces   | PE   |

**Table 55: Network Access Commands** (Continued)

| Command  | Function   | Mode |
|--|--|------|
| <code>show network-access mac-address-table</code> | Displays information for entries in the secure MAC address table | PE   |
| <code>show network-access mac-filter</code>        | Displays information for entries in the MAC filter tables        | PE   |

**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 256](#)).
- ◆ The maximum number of secure MAC addresses supported for the switch system is 1024.

### Example

```
Console(config-if)#network-access aging
Console(config-if)#
```

**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 56: Dynamic QoS Profiles**

| Profile    | Attribute Syntax                                   | Example                       |
|------------|--|-------------------------------|
| DiffServ   | <b>service-policy-in</b> = <i>policy-map-name</i>  | service-policy-in=p1          |
| Rate Limit | <b>rate-limit-input</b> = <i>rate</i> (kbps)       | rate-limit-input=100 (kbps)   |
|            | <b>rate-limit-output</b> = <i>rate</i> (kbps)      | rate-limit-output=200 (kbps)  |
| 802.1p     | <b>switchport-priority-default</b> = <i>value</i>  | switchport-priority-default=2 |
| IP ACL     | <b>ip-access-group-in</b> = <i>ip-acl-name</i>     | ip-access-group-in=ipv4acl    |
| IPv6 ACL   | <b>ipv6-access-group-in</b> = <i>ipv6-acl-name</i> | ipv6-access-group-in=ipv6acl  |
| MAC ACL    | <b>mac-access-group-in</b> = <i>mac-acl-name</i>   | mac-access-group-in=macAcl    |

- ◆ 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).
- ◆ EA port can only be assigned to the guest VLAN in case of failed authentication, if `switchport mode` is set to Hybrid.

#### 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 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

### 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*

**no 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**

*count* - The maximum number of MAC-authenticated MAC addresses allowed. (Range: 1-1024)

#### Default Setting

1024

#### Command Mode

Interface Configuration

#### Example

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

**clear network-access mac-address-table** 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 identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

#### 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: 1-12)

### 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              : Enabled

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: 1-12)

**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-00-00-00 would result in all MACs in the range 00-00-01-00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

### Example

```

Console#show network-access mac-address-table
Interface M@C Address      RADIUS Server  Time              Attribute
-----
1/1      00-00-01-02-03-04  172.155.120.17  00d06h32m50s     Static
1/1      00-00-01-02-03-05  172.155.120.17  00d06h33m20s     Dynamic
1/1      00-00-01-02-03-06  172.155.120.17  00d06h35m10s     Static
1/3      00-00-01-02-03-07  172.155.120.17  00d06h34m20s     Dynamic

Console#

```

**show network-access mac-filter** Use this command to display information for entries in the MAC filter tables.

**Syntax**

**show network-access mac-filter** [*filter-id*]

*filter-id* - Specifies a MAC address filter table. (Range: 1-64)

**Default Setting**

Displays all filters.

**Command Mode**

Privileged Exec

**Example**

```
Console#show network-access mac-filter
Filter ID MAC Address      MAC Mask
-----
      1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

---

## 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.



**Note:** RADIUS authentication must be activated and configured for the web authentication feature to work properly (see [“Authentication Sequence” on page 218](#)).

**Note:** Web authentication cannot be configured on trunk ports.

---

**Table 57: Web Authentication**

| Command                                  | Function  | Mode |
|--|---|------|
| <a href="#">web-auth login-attempts</a>  | Defines the limit for failed web authentication login attempts                            | GC   |
| <a href="#">web-auth quiet-period</a>    | Defines the amount of time to wait after the limit for failed login attempts is exceeded. | GC   |
| <a href="#">web-auth session-timeout</a> | Defines the amount of time a session remains valid  | GC   |

Table 57: Web Authentication (Continued)

| Command                                      | Function   | Mode |
|--|--|------|
| <code>web-auth system-auth-control</code>    | Enables web authentication globally for the switch   | GC   |
| <code>web-auth</code>                        | Enables web authentication for an interface  | IC   |
| <code>web-auth re-authenticate (Port)</code> | Ends all web authentication sessions on the port and forces the users to re-authenticate                             | PE   |
| <code>web-auth re-authenticate (IP)</code>   | Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate | PE   |
| <code>show web-auth</code>                   | Displays global web authentication parameters  | PE   |
| <code>show web-auth interface</code>         | Displays interface-specific web authentication parameters and statistics   | PE   |
| <code>show web-auth summary</code>           | Displays a summary of web authentication port parameters and statistics  | PE   |

**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

### Example

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

**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)

#### Default Setting

3600 seconds

#### Command Mode

Global Configuration

#### Example

```
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

```
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.

#### Example

```
Console(config-if)#web-auth
Console(config-if)#
```

**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* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

#### 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** *interface ip*

*interface* - Specifies a port interface.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*ip* - IPv4 formatted IP address

#### Default Setting

None

#### Command Mode

Privileged Exec

#### 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

```

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* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### Command Mode

Privileged Exec

### Example

```

Console#show web-auth interface ethernet 1/2
Web Auth Status      : Enabled

Host Summary

IP address      Web-Auth-State Remaining-Session-Time
-----
1.1.1.1         Authenticated  295
1.1.1.2         Authenticated  111
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

      System Auth Control      : Enabled
Port      Status      Authenticated Host Count
----      -
1/ 1      Disabled     0
1/ 2      Enabled       8
1/ 3      Disabled     0
1/ 4      Disabled     0
1/ 5      Disabled     0
:
:
```

## DHCP Snooping

DHCP 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 DHCP snooping.

**Table 58: DHCP Snooping Commands**

| Command   | Function   | Mode |
|---|--|------|
| <a href="#">ip dhcp snooping</a>                                      | Enables DHCP snooping globally   | GC   |
| <a href="#">ip dhcp snooping information option</a>                   | Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id  | GC   |
| <a href="#">ip dhcp snooping information policy</a>                   | Sets the information option policy for DHCP client packets that include Option 82 information  | GC   |
| <a href="#">ip dhcp snooping information option encode no-subtype</a> | Disables use of sub-type and sub-length for the CID/RID in Option 82 information   | GC   |
| <a href="#">ip dhcp snooping information option remote-id</a>         | Sets the remote ID to the switch's IP address, MAC address, arbitrary string, TR-101 compliant node identifier, or removes VLAN ID from the end of the TR101 field | GC   |
| <a href="#">ip dhcp snooping information policy</a>                   | Sets the information option policy for DHCP client packets that include Option 82 information  | GC   |
| <a href="#">ip dhcp snooping verify mac-address</a>                   | Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header   | GC   |
| <a href="#">ip dhcp snooping vlan</a>                                 | Enables DHCP snooping on the specified VLAN  | GC   |

Table 58: DHCP Snooping Commands (Continued)

| Command   | Function   | Mode |
|---|--|------|
| <code>ip dhcp snooping information option circuit-id</code> | Enables or disables the use of DHCP Option 82 information circuit-id suboption | IC   |
| <code>ip dhcp snooping trust</code>                         | Configures the specified interface as trusted                                  | IC   |
| <code>clear ip dhcp snooping binding</code>                 | Clears DHCP snooping binding table entries from RAM                            | PE   |
| <code>clear ip dhcp snooping database flash</code>          | Removes all dynamically learned snooping entries from flash memory.            | PE   |
| <code>ip dhcp snooping database flash</code>                | Writes all dynamically learned snooping entries to flash memory                | PE   |
| <code>show ip dhcp snooping</code>                          | Shows the DHCP snooping configuration settings                                 | PE   |
| <code>show ip dhcp snooping binding</code>                  | Shows the DHCP snooping binding table entries                                  | PE   |

**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 fire wall. 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:
  - 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 \(311\)](#)

[ip dhcp snooping trust \(313\)](#)

### 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 DHCP 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.
- ◆ DHCP Snooping Information Option 82 and DHCP Relay Information Option 82 (see [page 807](#)) cannot both be enabled at the same time.

### 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

**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, TR-101 compliant node identifier, or removes VLAN ID from end of TR101 field. 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}
```

**no 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)

**Default Setting**

MAC address: hexadecimal

**Command Mode**

Global Configuration

### Command Usage

The format for TR101 option 82 is: "<IP> eth <SID>/<PORT>[:<VLAN>]". Note that the SID (Switch ID) is always 0. By default the PVID is added to the end of the TR101 field for untagged packets. For tagged packets, the VLAN ID is always added. Use the **ip dhcp snooping information option remote-id tr101 no-vlan-field** command to remove the VLAN ID from the end of the TR101 field for untagged packets. Use the **no** form of this command to add the PVID for untagged packets at the end of the TR101 field.

### 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}**

**no ip dhcp snooping information policy**

**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 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 \(305\)](#)

[ip dhcp snooping vlan \(311\)](#)

[ip dhcp snooping trust \(313\)](#)

**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 \(305\)](#)

[ip dhcp snooping trust \(313\)](#)

### [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** *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` command.

- ◆ Option 82 information generated by the switch is based on TR-101 syntax as shown below:

**Table 59: Option 82 information**

| 82    | 3-69    | 1        | 1-67       | x1 | x2 | x3 | x4 | x5 | x63          |
|-------|---------|----------|------------|----|----|----|----|----|--------------|
| opt82 | opt-len | sub-opt1 | string-len |    |    |    |    |    | R-124 string |

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` 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 fire wall.
- ◆ Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall 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 \(305\)](#)

[ip dhcp snooping vlan \(311\)](#)

**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#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
Verify Source MAC-Address: enabled
Interface    Trusted    Circuit-ID mode  Circuit-ID Value
-----
Eth 1/1      No         VLAN-Unit-Port  ---
Eth 1/2      No         VLAN-Unit-Port  ---
Eth 1/3      No         VLAN-Unit-Port  ---
Eth 1/4      No         VLAN-Unit-Port  ---
Eth 1/5      No         VLAN-Unit-Port  ---
:
:
```

**show ip dhcp snooping binding** This command shows the DHCP snooping binding table entries.

**Command Mode**  
Privileged Exec

**Example**

```
Console#show ip dhcp snooping binding
MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
11-22-33-44-55-66 192.168.0.99    0           Dynamic-DHCPSNP  1    Eth 1/5
Console#
```

## IP Source Guard

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see [“DHCP Snooping” on page 304](#)). IP 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 IP Source Guard.

**Table 60: IP Source Guard Commands**

| Command                                 | Function   | Mode |
|---|--|------|
| <a href="#">ip source-guard binding</a> | Adds a static address to the source-guard binding table  | GC   |
| <a href="#">ip source-guard</a>         | Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address | IC   |

Table 60: IP Source Guard Commands

| Command                                   | Function   | Mode |
|---|--|------|
| <code>ip source-guard max-binding</code>  | Sets the maximum number of entries that can be bound to an interface | IC   |
| <code>show ip source-guard</code>         | Shows whether source guard is enabled or disabled on each interface  | PE   |
| <code>show ip source-guard binding</code> | Shows the source guard binding table                                 | PE   |

**ip 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

**ip source-guard binding** *mac-address* **vlan** *vlan-id* *ip-address*  
**interface ethernet** *unit/port*

**no ip source-guard binding** *mac-address* **vlan** *vlan-id*

*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 classful 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: 1-12)

### Default Setting

No configured entries

### Command Mode

Global Configuration

### Command Usage

- ◆ 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.
- ◆ 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.

- ◆ An entry with same MAC address and a different VLAN ID cannot be added to the binding table .
- ◆ Static bindings are processed as follows:
  - A valid static IP source guard entry will be added to the binding table in ACL mode if one of the following conditions is true:
    - 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.
  - Note that a static IP source guard entry cannot be added for a non-existent VLAN.
  - A valid static IP source guard entry will be added to the binding table in MAC mode if one of the following conditions are true:
    - If there is no binding entry with the same IP address and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding entry.
    - If there is a binding entry with same IP address and MAC address, then the new entry shall replace the old one.
- ◆ Only unicast addresses are accepted for static bindings.

### Example

This example configures a static source-guard binding on port 5.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99
interface ethernet 1/5
Console(config-if)#
```

### Related Commands

[ip source-guard \(319\)](#)

[ip dhcp snooping \(305\)](#)

[ip dhcp snooping vlan \(311\)](#)

**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 fire wall, 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 DHCP snooping is disabled (see [page 305](#)), 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 allowed by DHCP snooping.
- 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 \(317\)](#)

[ip dhcp snooping \(305\)](#)

[ip dhcp snooping vlan \(311\)](#)

**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 max-binding** *number*

**no ip source-guard max-binding**

*number* - The maximum number of IP 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 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.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
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
Interface  Filter-type  Max-binding
-----  -
Eth 1/1    DISABLED        5
Eth 1/2    DISABLED        5
Eth 1/3    DISABLED        5
Eth 1/4    DISABLED        5
Eth 1/5    SIP              1
Eth 1/6    DISABLED        5
:
```

**show ip source-guard binding** This command shows the source guard binding table.

### Syntax

**show ip source-guard binding [dhcp-snooping | static]**

**dhcp-snooping** - Shows dynamic entries configured with DHCP Snooping commands (see [page 304](#))

**static** - Shows static entries configured with the `ip source-guard binding` command (see [page 317](#)).

### Command Mode

Privileged Exec

### Example

```
Console#show ip source-guard binding
MAC Address      IP Address      Type           VLAN      Interface
-----
00-10-b5-f4-d0-01 10.2.44.96     static-acl     1 Eth 1/1
Console#
```

## 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 61: ARP Inspection Commands**

| Command   | Function   | Mode |
|---|--|------|
| <code>ip arp inspection</code>                    | Enables ARP Inspection globally on the switch  | GC   |
| <code>ip arp inspection filter</code>             | Specifies an ARP ACL to apply to one or more VLANs   | GC   |
| <code>ip arp inspection log-buffer logs</code>    | Sets the maximum number of entries saved in a log message, and the rate at these messages are sent             | GC   |
| <code>ip arp inspection validate</code>           | Specifies additional validation of address components in an ARP packet   | GC   |
| <code>ip arp inspection vlan</code>               | Enables ARP Inspection for a specified VLAN or range of VLANs  | GC   |
| <code>ip arp inspection limit</code>              | Sets a rate limit for the ARP packets received on a port   | IC   |
| <code>ip arp inspection trust</code>              | Sets a port as trusted, and thus exempted from ARP Inspection  | IC   |
| <code>show ip arp inspection configuration</code> | Displays the global configuration settings for ARP Inspection  | PE   |
| <code>show ip arp inspection interface</code>     | Shows the trust status and inspection rate limit for ports   | PE   |
| <code>show ip arp inspection log</code>           | Shows information about entries stored in the log, including the associated VLAN, port, and address components | PE   |

Table 61: ARP Inspection Commands (Continued)

| Command  | Function  | Mode |
|--|---|------|
| <code>show ip arp inspection statistics</code> | Shows statistics about the number of ARP packets processed, or dropped for various reasons  | PE   |
| <code>show ip arp inspection vlan</code>       | 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 | PE   |

**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 ACLs are configured with the commands described under “Configuring an ARP ACL” in the *Web Management Guide*.
- ◆ 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

```
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 [src-mac]] |  
  ip [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.

**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(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**

*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(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit 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           : 1 s
Log Message Number             : 5
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: 1-12)

**Command Mode**  
Privileged Exec

### Example

```

Console#show ip arp inspection interface ethernet 1/1

Port Number      Trust Status      Rate Limit (pps)
-----
Eth 1/1          Untrusted         15
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 : 0
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

### Command Usage

Enter this command to display the configuration settings for all VLANs, or display the settings for a specific VLAN by entering the VLAN identifier.

### Example

```

Console#show ip arp inspection vlan 1

VLAN ID      DAI Status      ACL Name      ACL Status
-----      -
1            disabled        sales         static
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 62: DoS Protection Commands**

| Command                                       | Function  | Mode |
|---|---|------|
| <code>dos-protection echo-charge</code>       | Protects against DoS echo/charge attacks  | GC   |
| <code>dos-protection smurf</code>             | Protects against DoS smurf attacks  | GC   |
| <code>dos-protection tcp-flooding</code>      | Protects against DoS TCP-flooding attacks   | GC   |
| <code>dos-protection tcp-null-scan</code>     | Protects against DoS TCP-null-scan attacks  | GC   |
| <code>dos-protection tcp-syn-fin-scan</code>  | Protects against DoS TCP-SYN/FIN-scan attacks                                     | GC   |
| <code>dos-protection tcp-udp-port-zero</code> | Protects against attacks which set the Layer 4 source or destination port to zero | GC   |
| <code>dos-protection tcp-xmas-scan</code>     | Protects against DoS TCP-XMAS-scan attacks  | GC   |
| <code>dos-protection udp-flooding</code>      | Protects against DoS UDP-flooding attacks   | GC   |
| <code>dos-protection win-nuke</code>          | Protects against DoS WinNuke attacks  | GC   |
| <code>show dos-protection</code>              | Shows the configuration settings for DoS protection                               | PE   |

**dos-protection echo-charge** This command protects against DoS echo/charge attacks in which the echo service repeats anything sent to it, and the charge (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

**[no] dos-protection echo-charge [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-charge 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

#### Example

```
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

**[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(config)#dos-protection tcp-flooding 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

### Command Usage

In these packets, all TCP flags are 0.

### 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 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

**[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

**[no] dos-protection win-nuke [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 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 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 63: Commands for Configuring Traffic Segmentation**

| Command  | Function   | Mode |
|--|--|------|
| <code>traffic-segmentation</code>                      | Enables traffic segmentation   | GC   |
| <code>traffic-segmentation session</code>              | Creates a client session   | GC   |
| <code>traffic-segmentation uplink/<br/>downlink</code> | Configures uplink/downlink ports for client sessions   | GC   |
| <code>traffic-segmentation<br/>uplink-to-uplink</code> | Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions | GC   |
| <code>show traffic-segmentation</code>                 | Displays the configured traffic segments   | PE   |

**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 64: Traffic Segmentation Forwarding**

| Destination Source               | Session #1 Downlinks | Session #1 Uplinks   | Session #2 Downlinks | Session #2 Uplinks   | Normal Ports |
|----------------------------------|----------------------|----------------------|----------------------|----------------------|--------------|
| <b>Session #1 Downlink Ports</b> | Blocking             | Forwarding           | Blocking             | Blocking             | Blocking     |
| <b>Session #1 Uplink Ports</b>   | Forwarding           | Forwarding           | Blocking             | Blocking/Forwarding* | Forwarding   |
| <b>Session #2 Downlink Ports</b> | Blocking             | Blocking             | Blocking             | Forwarding           | Blocking     |
| <b>Session #2 Uplink Ports</b>   | Blocking             | Blocking/Forwarding* | Forwarding           | Forwarding           | Forwarding   |
| <b>Normal Ports</b>              | Forwarding           | Forwarding           | Forwarding           | Forwarding           | Forwarding   |

\* 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] traffic-segmentation 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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 uplink-to-uplink** 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

Session  Uplink Ports          Downlink Ports
-----
   1     Ethernet 1/1          Ethernet 1/2
                                   Ethernet 1/3
                                   Ethernet 1/4

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, or 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 65: Access Control List Commands**

| Command Group   | Function  |
|-----------------|---|
| IPv4 ACLs       | Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code |
| IPv6 ACLs       | Configures ACLs based on IPv6 addresses, DSCP traffic class, or next header type                  |
| MAC ACLs        | Configures ACLs based on hardware addresses, packet format, and Ethernet type                     |
| ARP ACLs        | Configures ACLs based on ARP messages addresses   |
| ACL Information | Displays ACLs and associated rules; shows ACLs assigned to each port                              |

## 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 66: IPv4 ACL Commands**

| Command                           | Function  | Mode         |
|-----------------------------------|---|--------------|
| <code>access-list ip</code>       | Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs  | GC           |
| <code>permit, deny</code>         | Filters packets matching a specified source IPv4 address  | IPv4-STD-ACL |
| <code>permit, deny</code>         | Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code | IPv4-EXT-ACL |
| <code>ip access-group</code>      | Binds an IPv4 ACL to a port   | IC           |
| <code>show ip access-group</code> | Shows port assignments for IPv4 ACLs  | PE           |
| <code>show ip access-list</code>  | Displays the rules for configured IPv4 ACLs   | PE           |

**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

**[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 64 rules.

### Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

### Related Commands

[permit, deny \(345\)](#)

[ip access-group \(348\)](#)

[show ip access-list \(349\)](#)

**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: 1-16 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  
Console(config-std-acl)#
```

### Related Commands

[access-list ip \(344\)](#)

[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}  
  [dscp dscp] [precedence precedence]  
  [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}  
  [dscp dscp] [precedence precedence]  
  [source-port sport [bitmask]]  
  [destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp  
  {any | source address-bitmask | host source}  
  {any | destination address-bitmask | host destination}  
  [dscp dscp] [precedence precedence]  
  [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}  
  [dscp dscp] [precedence precedence]  
  [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.

*dscp* – DSCP priority level. (Range: 0-63)

*precedence* – IP precedence level. (Range: 0-7)

*sport* – Protocol<sup>4</sup> source port number. (Range: 0-65535)

*dport* – Protocol<sup>4</sup> 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: 1-16 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.
  
- ◆ 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
Console(config-ext-acl)#
```

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
Console(config-ext-acl)#
```

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
Console(config-ext-acl)#
```

### Related Commands

[access-list ip \(344\)](#)

[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 | out}
[time-range time-range-name] [counter]
```

```
no ip access-group acl-name {in | out}
```

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

**in** – Indicates that this list applies to ingress packets.

**out** – Indicates that this list applies to egress 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

- ◆ 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 \(349\)](#)

[Time Range \(155\)](#)

**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 \(348\)](#)

**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 \(345\)](#)

[ip access-group \(348\)](#)

## 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 67: IPv6 ACL Commands

| Command                                | Function  | Mode          |
|--|---|---------------|
| <a href="#">access-list ipv6</a>       | Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs  | GC            |
| <a href="#">permit, deny</a>           | Filters packets matching a specified source IPv6 address  | IPv6- STD-ACL |
| <a href="#">permit, deny</a>           | Filters packets meeting the specified criteria, including source or destination IPv6 address, DSCP traffic class, or next header type | IPv6- EXT-ACL |
| <a href="#">ipv6 access-group</a>      | Adds a port to an IPv6 ACL  | IC            |
| <a href="#">show ipv6 access-group</a> | Shows port assignments for IPv6 ACLs  | PE            |
| <a href="#">show ipv6 access-list</a>  | Displays the rules for configured IPv6 ACLs   | PE            |

**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 \(Standard IPv6 ACL\) \(351\)](#)  
[permit, deny \(Extended IPv6 ACL\) \(353\)](#)  
[ipv6 access-group \(356\)](#)  
[show ipv6 access-list \(357\)](#)

**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 \(350\)](#)

[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

```
[no] {permit | deny} next-header
    {any | host source-ipv6-address | source-ipv6-address[/prefix-length]}
    {any | destination-ipv6-address[/prefix-length]}
    [dscp dscp]
```

```
{permit | deny} udp
    {any | host source-ipv6-address | source-ipv6-address[/prefix-length]}
    {any | destination-ipv6-address[/prefix-length]}
    [dscp dscp] [next-header next-header]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
    [time-range time-range-name]
```

```
no {permit | deny} udp
    {any | host source-ipv6-address | source-ipv6-address[/prefix-length]}
    {any | destination-ipv6-address[/prefix-length]}
    [dscp dscp] [next-header next-header]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp
    {any | host source-ipv6-address | source-ipv6-address[/prefix-length]}
    {any | destination-ipv6-address[/prefix-length]}
    [dscp dscp]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
    [time-range time-range-name]
```

```
no {permit | deny} tcp
    {any | host source-ipv6-address | source-ipv6-address[/prefix-length]}
    {any | destination-ipv6-address[/prefix-length]}
    [dscp dscp]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
```

**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.

*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)

*sport* - Protocol<sup>5</sup> source port number. (Range: 0-65535)

*dport* - Protocol<sup>4</sup> 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

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) |

---

5. Includes TCP and UDP.

**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 from any source to any destination when the next header is 43..

```
Console(config-ext-ipv6-acl)#permit any any next-header 43
Console(config-ext-ipv6-acl)#
```

Here is a more detailed example for setting the CPU rate limit for SNMP packets.

```
Set ACL
Console(config)#access-list ip extended snmp-acl
Console(config-ext-acl)#permit UDP any any destination-port 161
Console(config-ext-acl)#permit UDP any any destination-port 162
Console(config-ext-acl)#exit

Set class map
Console(config)#class-map snmp-class
Console(config-cmap)#match access-list snmp-acl
Console(config-cmap)#

Set policy map and rate-limit
Console(config)#policy-map cpu-rate-limit-policy
Console(config-pmap)#class snmp-class
Console(config-pmap-c)police flow 10000 20000 conform-action transmit
    violate-action drop
Console(config-pmap-c)exit
Console(config-pmap)#exit

Bind the service-policy to control-plane
Console(config)#control-plane
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input cpu-rate-limit-policy
Console(config-if)#
```

**Related Commands**

[access-list ipv6 \(350\)](#)

[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 | out} [time-range time-range-name]  
[counter]
```

```
no ipv6 access-group acl-name {in | out}
```

*acl-name* – Name of the ACL. (Maximum length: 32 characters)

**in** – Indicates that this list applies to ingress packets.

**out** – Indicates that this list applies to egress 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.

### 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 \(357\)](#)

[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 \(356\)](#)

**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#
```

## Related Commands

[permit, deny \(Standard IPv6 ACL\) \(351\)](#)

[permit, deny \(Extended IPv6 ACL\) \(353\)](#)

[ipv6 access-group \(356\)](#)

## MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. 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 68: MAC ACL Commands**

| Command                            | Function  | Mode    |
|------------------------------------|---|---------|
| <code>access-list mac</code>       | Creates a MAC ACL and enters configuration mode   | GC      |
| <code>permit, deny</code>          | Filters packets matching a specified source and destination address, packet format, and Ethernet type | MAC-ACL |
| <code>mac access-group</code>      | Binds a MAC ACL to a port   | IC      |
| <code>show mac access-group</code> | Shows port assignments for MAC ACLs   | PE      |
| <code>show mac access-list</code>  | Displays the rules for configured MAC ACLs  | PE      |

**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/v6 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 \(359\)](#)  
[mac access-group \(361\)](#)  
[show mac access-list \(362\)](#)

**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}
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]] [time-range
  time-range-name]

no {permit | deny}
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [vid vid vid-bitmask] [ethertype protocol [protocol-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}
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]] [time-range
  time-range-name]

no {permit | deny} tagged-eth2
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]

{permit | deny} untagged-eth2
  {any | host source | source address-bitmask}
  {any | host destination | destination address-bitmask}
  [ethertype protocol [protocol-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]]
```

```
{permit | deny} tagged-802.3  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [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}  
  [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 address.

*destination* – Destination MAC address range with bitmask.

*address-bitmask*<sup>6</sup> – Bitmask for MAC address (in hexadecimal format).

*vid* – VLAN ID. (Range: 1-4094)

*vid-bitmask*<sup>6</sup> – VLAN bitmask. (Range: 1-4095)

*protocol* – A specific Ethernet protocol number. (Range: 0-ffff hex.)

*protocol-bitmask*<sup>6</sup> – Protocol bitmask. (Range: 0-ffff hex.)

*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.

---

6. For all bitmasks, “1” means care and “0” means ignore.

- ◆ 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 \(358\)](#)

[Time Range \(155\)](#)

**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 | out} [time-range time-range-name]
[counter]
```

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

**in** – Indicates that this list applies to ingress packets.

**out** – Indicates that this list applies to egress 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 \(362\)](#)  
[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 \(361\)](#)

**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 \(359\)](#)  
[mac access-group \(361\)](#)

## 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.

**Table 69: ARP ACL Commands**

| Command                           | Function   | Mode    |
|-----------------------------------|--|---------|
| <code>access-list arp</code>      | Creates a ARP ACL and enters configuration mode                                    | GC      |
| <code>permit, deny</code>         | Filters packets matching a specified source or destination address in ARP messages | ARP-ACL |
| <code>show access-list arp</code> | Displays the rules for configured ARP ACLs   | PE      |

**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 \(364\)](#)

[show access-list arp \(365\)](#)

**permit, deny (ARPA CL)** 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.

*ip-address-bitmask*<sup>7</sup> – IPv4 number representing the address bits to match.

*source-mac* – Source MAC address.

*destination-mac* – Destination MAC address range with bitmask.

*mac-address-bitmask*<sup>7</sup> – 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  
Console(config-mac-acl)#
```

7. For all bitmasks, binary “1” means relevant and “0” means ignore.

## Related Commands

[access-list arp \(363\)](#)

**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#
```

## Related Commands

[permit, deny \(364\)](#)

---

## ACL Information

This section describes commands used to display ACL information.

**Table 70: ACL Information Commands**

| Command   | Function   | Mode |
|---|--|------|
| <a href="#">clear access-list hardware counters</a> | Clears hit counter for rules in all ACLs, or in a specified ACL. | PE   |
| <a href="#">show access-group</a>                   | Shows the ACLs assigned to each port                             | PE   |
| <a href="#">show access-list</a>                    | Show all ACLs and associated rules                               | PE   |

**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.

**out** – Clears counter for egress rules.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*acl-name* – Name of the ACL. (Maximum length: 32 characters)

### Command Mode

Privileged Exec

### Example

```
Console#clear access-list hardware counters
Console#
```

**show access-group** This command shows the port assignments of ACLs.

### Command Mode

Privileged Executive

### Example

```
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

#### **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.<sup>8</sup>

**ip extended** – Shows ingress or egress rules for Extended IPv4 ACLs.

**ip standard** – Shows ingress or egress rules for Standard IPv4 ACLs.

**ipv6 extended** – Shows ingress or egress rules for Extended IPv6 ACLs.

**ipv6 standard** – Shows ingress or egress rules for Standard IPv6 ACLs.

8. Due to a hardware limitation, this option only displays statistics for permit rules.

**mac** – Shows ingress or egress 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 71: Interface Commands**

| Command                                 | Function  | Mode   |
|---|---|--------|
| <i>Interface Configuration</i>          |   |        |
| <code>interface</code>                  | Configures an interface type and enters interface configuration mode  | GC     |
| <code>alias</code>                      | Configures an alias name for the interface  | IC     |
| <code>capabilities</code>               | Advertises the capabilities of a given interface for use in autonegotiation   | IC     |
| <code>description</code>                | Adds a description to an interface configuration  | IC     |
| <code>discard</code>                    | Discards CDP or PVST packets  | IC     |
| <code>flowcontrol</code>                | Enables flow control on a given interface   | IC     |
| <code>history</code>                    | Configures a periodic sampling of statistics, specifying the sampling interval and number of samples                                    | IC     |
| <code>media-type</code>                 | Force port type selected for combination ports  | IC     |
| <code>negotiation</code>                | Enables autonegotiation of a given interface  | IC     |
| <code>shutdown</code>                   | Disables an interface   | IC     |
| <code>speed-duplex</code>               | Configures the speed and duplex operation of a given interface when autonegotiation is disabled   | IC     |
| <code>clear counters</code>             | Clears statistics on an interface   | PE     |
| <code>show discard</code>               | Displays if CDP and PVST packets are being discarded  | PE     |
| <code>show interfaces brief</code>      | Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type | PE     |
| <code>show interfaces counters</code>   | Displays statistics for the specified interfaces  | NE, PE |
| <code>show interfaces history</code>    | Displays statistical history for the specified interfaces   | PE     |
| <code>show interfaces status</code>     | Displays status for the specified interface   | NE, PE |
| <code>show interfaces switchport</code> | Displays the administrative and operational status of an interface  | NE, PE |

**Table 71: Interface Commands** (Continued)

| Command  | Function  | Mode |
|--|---|------|
| <i>Transceiver Threshold Configuration</i>         |   |      |
| <code>transceiver-monitor</code>                   | Sends a trap when any of the transceiver's operational values fall outside specified thresholds                         | IC   |
| <code>transceiver-threshold-auto</code>            | Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent | IC   |
| <code>transceiver-threshold current</code>         | Sends a trap when the transceiver current falls outside the specified thresholds  | IC   |
| <code>transceiver-threshold rx-power</code>        | Sends a trap when the power level of the received signal falls outside the specified thresholds                         | IC   |
| <code>transceiver-threshold temperature</code>     | Sends a trap when the transceiver temperature falls outside the specified thresholds                                    | IC   |
| <code>transceiver-threshold tx-power</code>        | Sends a trap when the power level of the transmitted signal power outside the specified thresholds                      | IC   |
| <code>transceiver-threshold voltage</code>         | Sends a trap when the transceiver voltage falls outside the specified thresholds  | IC   |
| <code>show interfaces transceiver</code>           | Displays the temperature, voltage, bias current, transmit power, and receive power                                      | PE   |
| <code>show interfaces transceiver-threshold</code> | Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power         | PE   |
| <i>Cable Diagnostics</i>                           |   |      |
| <code>test cable-diagnostics</code>                | Performs cable diagnostics on the specified port  | PE   |
| <code>show cable-diagnostics</code>                | Shows the results of a cable diagnostics test   | PE   |
| <i>Power Savings</i>                               |   |      |
| <code>power-save</code>                            | Enables power savings mode on the specified port  | IC   |
| <code>show power-save</code>                       | 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. Use the **no** form with a Layer 3 VLAN (normal type) to change it back to a Layer 2 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.

**craft** - Management port on the front panel.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Physical port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**vlan** *vlan-id* (Range: 1-4094)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

The craft interface is provided as an out-of-band management connection which is isolated from all other ports on the switch. This interface must first be configured with an IPv4 or IPv6 address before a connection can be made through Telnet, SSH, or HTTP.

### Example

To specify several different ports, enter the following command:

```
Console(config)#interface ethernet 1/17-20,23
Console(config-if)#
```

**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 {1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric}**

**1000full** - Supports 1 Gbps full-duplex operation

**100full** - Supports 100 Mbps full-duplex operation

**100half** - Supports 100 Mbps half-duplex operation

**10full** - Supports 10 Mbps full-duplex operation

**10half** - Supports 10 Mbps half-duplex operation

**flowcontrol** - Supports flow control

**symmetric** (Gigabit only) - When specified, the port transmits and receives symmetric pause frames.

### Default Setting

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/LH (SFP): 1000full

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

### Related Commands

[negotiation \(376\)](#)

[speed-duplex \(378\)](#)

[flowcontrol \(374\)](#)

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

**discard** This command discards CDP or PVST packets. Use the **no** form to forward the specified packet type to other ports configured the same way.

### Syntax

**[no] discard {cdp | pvst}**

**cdp** – Cisco Discovery Protocol

**pvst** – Per-VLAN Spanning Tree

### Default Setting

Default - Forward CDP and PVST packets

### Command Mode

Interface Configuration (Ethernet)

### Command Usage

Use the **no discard** command to allow CDP or PVST packets to be forwarded to other ports in the same VLAN which are also configured to forward the specified packet type.

### Example

The following example forwards CDP packets entering port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no discard cdp
Console(config-if)#
```

**flowcontrol** This command enables flow control. Use the **no** form to disable flow control.

### Syntax

**[no] flowcontrol**

### Default Setting

Disabled

### 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.
- ◆ Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, 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 \(376\)](#)

[capabilities \(flowcontrol, symmetric\) \(372\)](#)

**history** This command configures a periodic sampling of statistics, specifying the sampling interval and number of samples. Use the **no** form to remove a named entry from the sampling table.

### Syntax

**history** *name interval buckets*

**no history** *name*

*name* - A symbolic name for this entry in the sampling table. (Range: 1-32 characters)

*interval* - The interval for sampling statistics. (Range: 1-1440 minutes.)

*buckets* - The number of samples to take. (Range: 1-96)

### Default Setting

15min - 15 minute interval, 96 buckets

1day - 1 day interval, 7 buckets

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Example

This example sets a interval of 15 minutes for sampling standard statistical values on port 1.

```
Console(config)#interface ethernet 1/1  
Console(config-if)#history 15min 15 10  
Console(config-if)#
```

**media-type** This command forces the port type selected for combination ports. Use the **no** form to restore the default mode.

### Syntax

**media-type {copper-forced | sfp-forced [*mode*] | sfp-preferred-auto}**

**no media-type**

*mode*

**copper-forced** - Always uses the built-in RJ-45 port.

**sfp-forced** - Always uses the SFP port (even if module not installed).

**sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

*mode*

**1000sfp** - Always uses 1000BASE SFP mode.

**100fx** - Always uses 100BASE-FX mode.

### Default Setting

sfp-preferred-auto

### Command Mode

Interface Configuration (Ethernet)

### Example

This forces the switch to use the built-in RJ-45 port for the combination port 10.

```
Console(config)#interface ethernet 1/10  
Console(config-if)#media-type copper-forced  
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 10 to use auto-negotiation.

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

### Related Commands

[capabilities \(372\)](#)

[speed-duplex \(378\)](#)

**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** {**1000full** | **100full** | **100half** | **10full** | **10half**}

**no speed-duplex**

**1000full** - Forces 1000 Mbps 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.

### 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.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

### Related Commands

[negotiation \(376\)](#)

[capabilities \(372\)](#)

**clear counters** This command clears statistics on an interface.

### Syntax

**clear counters** *interface*

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**vlan** *vlan-id* (Range: 1-4094)

### 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.

```
Console#clear counters ethernet 1/5
Console#
```

**show discard** This command displays whether or not CDP and PVST packets are being discarded.

### Command Mode

Privileged Exec

### Example

In this example, "Default" means that the packets are not discarded.

```
Console#show discard
Port      CDP      PVST
-----
Eth 1/ 1  Default Default
Eth 1/ 2  Default Default
Eth 1/ 3  Default Default
Eth 1/ 4  Default Default
Eth 1/ 5  Default Default
Eth 1/ 6  Default Default
:
```

**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.
- ◆ If link status is down due to an administrative setting or the result of a protocol state, the reason will be listed in the Status field (i.e., STP LBD, BpduGuard, LinkDet, DynQoS, PortSec, LBD, ATC Bcast, ATC Mcast, UDLD).

### Example

```
Console#show interfaces brief
Interface Name      Status   PVID Pri Speed/Duplex  Type      Trunk
-----
Eth 1/ 1           Up       1   0 Auto-100full  100TX     None
Eth 1/ 2           BpduGuard 1   0 Auto         100TX     None
Eth 1/ 3           Down     1   0 Auto         100TX     None
Eth 1/ 4           Down     1   0 Auto         100TX     None
Eth 1/ 5           Down     1   0 Auto         100TX     None
```

```
Eth 1/ 6          Down          1    0 Auto          100TX          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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**vlan** *vlan-id* (Range: 1-4094)

### 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.

### Example

```
Console#show interfaces counters ethernet 1/1
Ethernet 1/ 1
===== 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 =====
1 Octets Input in kbits per second
1 Packets Input per second
0.00 % Input Utilization (
5 Octets Output in kbits per second
0 Packets Output per second
0.00 % Output Utilization

Console#show interfaces counters vlan 1
VLAN 1
21462 Octets Input
93 Packets Input

Console#

```

**Table 72: show interfaces counters - display description**

| Parameter             | Description   |
|-----------------------|---|
| <i>IF Table Stats</i> |   |
| Octets Input          | The total number of octets received on the interface, including framing characters.   |
| Octets Output         | The total number of octets transmitted out of the interface, including framing characters.  |
| Unicast Input         | The number of subnetwork-unicast packets delivered to a higher-layer protocol.  |
| Unicast Output        | The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.  |
| Discard Input         | The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |

**Table 72: show interfaces counters - display description** (Continued)

| Parameter                      | Description   |
|--------------------------------|---|
| Discard Output                 | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| Error Input                    | The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.  |
| Error Output                   | The number of outbound packets that could not be transmitted because of errors.   |
| Unknown Protocols Input        | The number of packets received which were discarded because of an unknown or unsupported protocol.  |
| QLen Output                    | The length of the output packet queue (in packets).   |
| <i>Extended IF Table Stats</i> |   |
| Multicast Input                | The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.  |
| Multicast Output               | The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.                           |
| Broadcast Input                | The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.  |
| Broadcast Output               | The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.                           |
| <i>Etherlike Statistics</i>    |   |
| Alignment Errors               | The number of alignment errors (missynchronized data packets).  |
| FCS Errors                     | A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.   |
| Single Collision Frames        | The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.   |
| Multiple Collision Frames      | A count of successfully transmitted frames for which transmission is inhibited by more than one collision.  |
| SQE Test Errors                | A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.   |
| Deferred Transmissions         | A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.  |
| Late Collisions                | The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.  |
| Excessive Collisions           | A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.                                      |
| Internal MAC Transmit Errors   | A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.  |
| Internal MAC Receive Errors    | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.  |
| Frames Too Long                | A count of frames received on a particular interface that exceed the maximum permitted frame size.  |

**Table 72: show interfaces counters - display description** (Continued)

| Parameter              | Description   |
|------------------------|---|
| Carrier Sense Errors   | The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.  |
| Symbol Errors          | For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present.<br><br>For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII.<br><br>For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII |
| <i>RMON Statistics</i> |   |
| Octets                 | Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.  |
| Packets                | The total number of packets (bad, broadcast and multicast) received.  |
| Broadcast Packets      | The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.   |
| Multicast Packets      | The total number of good packets received that were directed to this multicast address.   |
| Undersize Packets      | The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.  |
| Oversize Packets       | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.   |
| Fragments              | The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.  |
| Jabbers                | The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.   |
| CRC Align Errors       |   |
| Collisions             | The best estimate of the total number of collisions on this Ethernet segment.   |
| 64 Octets              | The total number of packets (including bad packets) received and transmitted that were less than 64 octets in length (excluding framing bits but including FCS octets).   |
| 65-127 Octets          | The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).  |
| 128-255 Octets         |   |
| 256-511 Octets         |   |
| 512-1023 Octets        |   |
| 1024-1518 Octets       |   |
| 1519-1536 Octets       |   |

**Table 72: show interfaces counters - display description** (Continued)

| Parameter                     | Description  |
|-------------------------------|--|
| <i>Utilization Statistics</i> |  |
| Octets input per second       | Number of octets entering this interface in kbits per second.    |
| Packets input per second      | Number of packets entering this interface in packets per second. |
| Input utilization             | The input utilization rate for this interface.                   |
| Octets output per second      | Number of octets leaving this interface in kbits per second.     |
| Packets output per second     | Number of packets leaving this interface in packets per second.  |
| Output utilization            | The output utilization rate for this interface.                  |

**show interfaces history** This command displays statistical history for the specified interfaces.

**show interfaces history** [*interface* [*name* [**current** | **previous** *index count*] [**input** | **output**]]]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*name* - Name of sample as defined in the [history](#) command. (Range: 1-32 characters)

**current** - Statistics recorded in current interval.

**previous** - Statistics recorded in previous intervals.

*index* - An index into the buckets containing previous samples. (Range: 1-96)

*count* - The number of historical samples to display. (Range: 1-96)

**input** - Ingress traffic.

**output** - Egress traffic.

#### Default Setting

Shows historical statistics for all interfaces, intervals, ingress traffic, and egress traffic.

#### Command Mode

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 *Web Management Guide*.

### Example

This example shows the statistics recorded for all named entries in the sampling table.

```

Console#show interfaces history ethernet 1/1
Interface      : Eth 1/ 1
Name           : 1min
Interval      : 1 minute(s)
Buckets Requested : 15
Buckets Granted  : 15
Status        : Active

Current Entries

Start Time   Octets Input   Unicast       Multicast     Broadcast
-----
00d 02:50:52      15059355      80275         43750         2304

Discards     Errors         Unknown Proto
-----
0             0             0

Octets Output Unicast       Multicast     Broadcast
-----
84493398     106787        47232         1158

Discards     Errors
-----
0             0

Interface    : Eth 1/ 1
Name         : 15min
Interval    : 15 minute(s)
Buckets Requested : 96
Buckets Granted  : 11
Status      : Active

Current Entries

Start Time   Octets Input   Unicast       Multicast     Broadcast
-----
00d 02:45:07      116003318     616894        336491        17899

Discards     Errors         Unknown Proto
-----
0             0             0

Octets Output Unicast       Multicast     Broadcast
-----
648387890    819696        358285        8921

Discards     Errors
-----
0             0

Interface    : Eth 1/ 1
Name         : 1day

```

```
Interval          : 1440 minute(s)
Buckets Requested : 7
Buckets Granted  : 0
Status           : Active
```

Current Entries

| Start Time   | Octets Input  | Unicast  | Multicast | Broadcast     |
|--------------|---------------|----------|-----------|---------------|
| 00d 00:00:01 | 1563328011    | 8391643  | 4440171   | 241090        |
|              |               | Discards | Errors    | Unknown Proto |
|              |               | 0        | 0         | 0             |
|              | Octets Output | Unicast  | Multicast | Broadcast     |
|              | 8896498997    | 11151669 | 4734465   | 119595        |
|              |               | Discards | Errors    |               |
|              |               | 0        | 0         |               |

Console#

This example shows the statistics recorded for a named entry in the sampling table.

```
Console#show interfaces history ethernet 1/1 1min
Interface       : Eth 1/ 1
Name            : 1min
Interval        : 1 minute(s)
Buckets Requested : 10
Buckets Granted  : 3
Status          : Active
```

Current Entries

| Start Time   | Octets Input  | Unicast  | Multicast | Broadcast     |
|--------------|---------------|----------|-----------|---------------|
| 00d 00:08:40 | 1042759       | 6932     | 1653      | 54            |
|              |               | Discards | Errors    | Unknown Proto |
|              |               | 0        | 0         | 0             |
|              | Octets Output | Unicast  | Multicast | Broadcast     |
|              | 5095864       | 7894     | 1776      | 18            |
|              |               | Discards | Errors    |               |
|              |               | 0        | 0         |               |

Previous Entries

| Start Time   | Octets Input | Unicast | Multicast | Broadcast |
|--------------|--------------|---------|-----------|-----------|
| 00d 00:05:37 | 1400912      | 9381    | 1895      | 50        |
| 00d 00:06:37 | 1566090      | 10660   | 2195      | 50        |
| 00d 00:07:37 | 1754781      | 11786   | 2674      | 59        |

| Start Time   | Octets Input | Discards | Errors | Unknown Proto |
|--------------|--------------|----------|--------|---------------|
| 00d 00:05:37 | 1400912      |          | 0      | 0             |
| 00d 00:06:37 | 1566090      |          | 0      | 0             |
| 00d 00:07:37 | 1754781      |          | 0      | 0             |

| Start Time   | Octets Output | Unicast | Multicast | Broadcast |
|--------------|---------------|---------|-----------|-----------|
| 00d 00:05:37 | 6827866       | 10563   | 2042      | 30        |
| 00d 00:06:37 | 7572668       | 12040   | 2362      | 30        |
| 00d 00:07:37 | 8548505       | 13380   | 2879      | 30        |

| Start Time   | Octets Output | Discards | Errors |
|--------------|---------------|----------|--------|
| 00d 00:05:37 | 6827866       |          | 0      |
| 00d 00:06:37 | 7572668       |          | 0      |
| 00d 00:07:37 | 8548505       |          | 0      |

**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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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 1/1
Basic Information:
  Port Type           : 1000BASE-T
  MAC Address         : 70-72-CF-59-8F-41
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : @uto

Capabilities          : 10half, 10full, 100half, 100full, 1000full
  
```

```

Broadcast Storm          : Enabled
Broadcast Storm Limit   : 64 kbits/second
Multicast Storm         : Disabled
Multicast Storm Limit   : 64 kbits/second
Unknown Unicast Storm   : Disabled
Unknown Unicast Storm Limit : 64 kbits/second
Flow Control            : Disabled
VLAN Trunking           : Disabled
LACP                    : Disabled
Media Type               : SFP preferred auto
Current Status:
Link Status              : Up
Port Operation Status    : Up
Operapion Speed-duplex  : 100full
Up Time                  : 0w 0d 7h 40m 23s (27623 seconds)
Flow Control Type       : None
Max Frame Size          : 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status     : Enabled
Console#

```

**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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 1.

```

Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
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       : Disabled
802.1Q Tunnel Mode         : Normal
802.1Q Tunnel TPID         : 8100 (Hex)
Layer 2 Protocol Tunnel    : None
Console#

```

**Table 73: show interfaces switchport - display description**

| Field                         | Description   |
|-------------------------------|---|
| Broadcast Threshold           | Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level ( <a href="#">page 429</a> ).       |
| Multicast Threshold           | Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level ( <a href="#">page 429</a> ).       |
| Unknown-unicast Threshold     | Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level ( <a href="#">page 429</a> ). |
| LACP Status                   | Shows if Link Aggregation Control Protocol has been enabled or disabled ( <a href="#">page 406</a> ).   |
| Ingress/Egress Rate Limit     | Shows if rate limiting is enabled, and the current rate limit ( <a href="#">page 867</a> ).   |
| VLAN Membership Mode          | Indicates membership mode as Trunk or Hybrid ( <a href="#">page 533</a> ).  |
| Ingress Rule                  | Shows if ingress filtering is enabled or disabled ( <a href="#">page 532</a> ).   |
| Acceptable Frame Type         | Shows if acceptable VLAN frames include all types or tagged frames only ( <a href="#">page 530</a> ).   |
| Native VLAN                   | Indicates the default Port VLAN ID ( <a href="#">page 534</a> ).  |
| Priority for Untagged Traffic | Indicates the default priority for untagged frames ( <a href="#">page 570</a> ).  |
| GVRP Status                   | Shows if GARP VLAN Registration Protocol is enabled or disabled ( <a href="#">page 525</a> ).   |
| Allowed VLAN                  | Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged ( <a href="#">page 531</a> ).            |
| Forbidden VLAN                | Shows the VLANs this interface can not dynamically join via GVRP ( <a href="#">page 524</a> ).  |
| 802.1Q Tunnel Status          | Shows if 802.1Q tunnel is enabled on this interface ( <a href="#">page 538</a> ).   |
| 802.1Q Tunnel Mode            | Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink ( <a href="#">page 539</a> ).  |
| 802.1Q Tunnel TPID            | Shows the Tag Protocol Identifier used for learning and switching packets ( <a href="#">page 542</a> ).                                       |
| Layer 2 Protocol Tunnel       | Shows specified protocol encapsulated by Layer 2 Protocol Tunneling ( <a href="#">page 547</a> ).   |

## 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

**[no] transceiver-monitor**

### Default Setting

Disabled

### Command Mode

Interface Configuration (SFP Ports)

### Example

```
Console(config)#interface ethernet 1/25
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 (SFP/SFP+ 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. Use the **no** form to restore the default settings.

### Syntax

**transceiver-threshold current** {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

**no transceiver-threshold current**

**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 (SFP 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.

```
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. Use the **no** form to restore the default settings.

### Syntax

**transceiver-threshold rx-power {high-alarm | high-warning | low-alarm | low-warning} *threshold-value***

**no transceiver-threshold rx-power**

**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)

### 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 (SFP 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. Use the **no** form to restore the default settings.

### Syntax

**transceiver-threshold temperature {high-alarm | high-warning | low-alarm | low-warning} threshold-value**

**no transceiver-threshold temperature**

**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 (SFP 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#
```

**transceiver-threshold tx-power** This command sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message. Use the **no** form to restore the default settings.

### Syntax

**transceiver-threshold tx-power {high-alarm | high-warning | low-alarm | low-warning} *threshold-value***

**no transceiver-threshold tx-power**

**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: -12.00 dBm

Low Alarm: -11.50 dBm

### Command Mode

Interface Configuration (SFP 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.

```
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. Use the **no** form to restore the default settings.

### Syntax

**transceiver-threshold voltage** {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

**no transceiver-threshold voltage**

**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

High Alarm: 3.50 Volts

High Warning: 3.45 Volts

Low Warning: 3.15 Volts

Low Alarm: 3.10 Volts

### Command Mode

Interface Configuration (SFP 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. (Range: SFP ports 1-12)

### 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 1/2
Information of Eth 1/12
Connector Type       : LC
Fiber Type           : Single Mode (SM)
Eth Compliance Codes : 1000BASE-LX
Baud Rate            : 1200 Mbd
Vendor OUI           : 00-17-6A
Vendor Name          : AVAGO
Vendor PN            : AFCT-5705APZ
Vendor Rev           : 0000
Vendor SN            : AC1119S00XU
Date Code            : 11-05-13
DDM Info
```

```
Temperature          : 37.86 degree C
Vcc                  : 3.30 V
Bias Current         : 13.11 mA
TX Power             : -6.61 dBm
RX Power             : -40.00 dBm
DDM Thresholds
-----
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#
```

**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. (Range: SFP ports 1-12)

### 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 1/12
Information of Eth 1/12
DDM Thresholds
Transceiver-monitor      : Disabled
Transceiver-threshold-auto : Disabled
-----
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: 1-12)

**Command Mode**

Privileged Exec

**Command Usage**

- ◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test methods. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- ◆ This cable test is only accurate for Ethernet cables 7 - 100 meters long.
- ◆ The test takes approximately 5 seconds. Use the [show cable-diagnostics](#) command to display the results of the test, including common cable failures, as well as the status and approximate length of each cable pair.
- ◆ 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 1/10  
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: 1-12)

### 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.
- ◆ 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 any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
  - Impedance mismatch: Terminating impedance is not in the reference range.

## Example

```

Console#show cable-diagnostics interface ethernet 1/10
TF: Test failed
OK: OK
ON: Open
ST: Short
IE: Impedance error
NC: No cable
NT: Not tested
NS: Not supported
UN: Unknown
Port      Type Link      Pair A   Pair B   Pair C   Pair D   Last
          Status meters meters meters meters meters Updated
-----
Eth 1/2 GE   Down    NC (0)  NC (0)  NC (0)  NC (0)  2000-12-31 08:28:59
Console#

```

## Power Savings

**power-save** This command enables power savings mode on the specified port. Use the **no** form to disable this feature.

### Syntax

**[no] power-save**

### Default Setting

Enabled

### Command Mode

Interface Configuration (Ethernet)

### 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 mode on a active link only works when the connection speed is 100 Mbps or higher at linkup, and line length is less than 60 meters.

### Example

```
Console(config)#interface ethernet 1/10
Console(config-if)#power-save
Console(config-if)#
```

**show power-save** This command shows the configuration settings for power savings.

### Syntax

**show power-save** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### Command Mode

Privileged Exec

### Example

```
Console#show power-save interface ethernet 1/10
Power Saving Status:
 Ethernet 1/10 : Enabled
Console#
```

# Link 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 74: Link Aggregation Commands**

| Command  | Function   | Mode              |
|--|--|-------------------|
| <i>Manual Configuration Commands</i>             |  |                   |
| <code>interface port-channel</code>              | Configures a trunk and enters interface configuration mode for the trunk | GC                |
| <code>port channel load-balance</code>           | Sets the load-distribution method among ports in aggregated links        | GC                |
| <code>channel-group</code>                       | Adds a port to a trunk   | IC (Ethernet)     |
| <i>Dynamic Configuration Commands</i>            |  |                   |
| <code>lacp</code>                                | Configures LACP for the current interface                                | IC (Ethernet)     |
| <code>lacp admin-key</code>                      | Configures a port's administration key                                   | IC (Ethernet)     |
| <code>lacp port-priority</code>                  | Configures a port's LACP port priority                                   | IC (Ethernet)     |
| <code>lacp system-priority</code>                | Configures a port's LACP system priority                                 | IC (Ethernet)     |
| <code>lacp admin-key</code>                      | Configures an port channel's administration key                          | IC (Port Channel) |
| <code>lacp timeout</code>                        | Configures the timeout to wait for next LACPDU                           | IC (Port Channel) |
| <i>Trunk Status Display Commands</i>             |  |                   |
| <code>show interfaces status port-channel</code> | Shows trunk information  | NE, PE            |
| <code>show lacp</code>                           | Shows LACP information   | PE                |
| <code>show port-channel load-balance</code>      | Shows the load-distribution method used on aggregated links              | PE                |

## 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 load-balance** 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-mac

## 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

**channel-group** *channel-id*

**no channel-group**

*channel-id* - Trunk index (Range: 1-12)

#### 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 10:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
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

**[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 1-3. 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 1/1
Console(config-if)#lACP
Console(config-if)#interface ethernet 1/2
Console(config-if)#lACP
Console(config-if)#interface ethernet 1/3
Console(config-if)#lACP
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic Information:
  Port Type           : 1000BASE-T
  MAC Address         : 70-72-CF-1C-BA-53
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : Auto
  Capabilities         : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 64 kbits/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 64 kbits/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 64 kbits/second
  Flow Control         : Disabled
  VLAN Trunking       : Disabled
Current status:
  Created By          : LACP
  Link Status         : Up
  Port Operation Status : Up
  Operation speed-duplex : 1000full
  Up Time             : 0w 0d 0h 0m 48s (48 seconds)
  Flow Control Type    : None
  Max Frame Size      : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status : Enabled
  Member Ports        : Eth1/1, Eth1/2, Eth1/3,
  Active Member Ports : Eth1/1, Eth1/2, Eth1/3,
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

**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.



**Note:** Configuring the partner admin-key does not affect remote or local switch operation. The local switch just records the partner admin-key for user reference.

- ◆ 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

```
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.
- ◆ 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 ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

**lacp admin-key** (Port Channel) 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.

### 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**

**long** - Specifies a slow timeout of 90 seconds.

**short** - Specifies a fast timeout of 3 seconds.

### 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** | **sysid**}

*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.

**sysid** - Summary of system priority and MAC address for all channel groups.

### Default Setting

Port Channel: all

### Command Mode

Privileged Exec

### Example

```

Console#show lacp 1 counters
Port Channel: 1
-----
Eth 1/ 2
-----
LACPDU Sent      : 12
LACPDU Received  : 6
Marker Sent      : 0
Marker Received  : 0
LACPDU Unknown Pkts : 0
LACPDU Illegal Pkts : 0
:

```

**Table 75: show lacp counters - display description**

| Field               | Description  |
|---------------------|--|
| LACPDU Sent         | Number of valid LACPDU transmitted from this channel group.  |
| LACPDU Received     | Number of valid LACPDU received on this channel group.   |
| Marker Sent         | Number of valid Marker PDU transmitted from this channel group.  |
| Marker Received     | Number of valid Marker PDU received by this channel group.   |
| LACPDU Unknown Pkts | 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. |
| LACPDU Illegal Pkts | Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.  |

```

Console#show lacp 1 internal
Port Channel : 1
-----
Oper Key : 3
Admin Key : 0
Timeout : long
Eth 1/ 1
-----
LACPDU 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 76: show lacp internal - display description**

| Field     | Description  |
|-----------|--|
| Oper Key  | Current operational value of the key for the aggregation port.             |
| Admin Key | Current administrative value of the key for the aggregation port.          |
| Timeout   | Time to wait for the next LACPDU before deleting partner port information. |

**Table 76: show lacp internal - display description** (Continued)

| Field                   | Description   |
|-------------------------|---|
| LACPDU Internal         | Number of seconds before invalidating received LACPDU information.  |
| LACP System Priority    | LACP system priority assigned to this port channel.   |
| LACP Port Priority      | LACP port priority assigned to this interface within the channel group.   |
| Admin State, Oper State | <p>Administrative or operational values of the actor's state parameters:</p> <ul style="list-style-type: none"> <li>◆ Expired – The actor's receive machine is in the expired state;</li> <li>◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner.</li> <li>◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information.</li> <li>◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information.</li> <li>◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.</li> <li>◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation.</li> <li>◆ Long timeout – Periodic transmission of LACPDU uses a slow transmission rate.</li> <li>◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)</li> </ul> |

```

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,
Oper State:                distributing, collecting, synchronization,
                             aggregation, long timeout, LACP-activity
:

```

**Table 77: show lacp neighbors - display description**

| Field                     | Description   |
|---------------------------|---|
| Partner Admin System ID   | LAG partner's system ID assigned by the user.   |
| Partner Oper System ID    | LAG partner's system ID assigned by the LACP protocol.                                    |
| Partner Admin Port Number | Current administrative value of the port number for the protocol Partner.                 |
| Partner Oper Port Number  | Operational port number assigned to this aggregation port by the port's protocol partner. |
| Port Admin Priority       | Current administrative value of the port priority for the protocol partner.               |
| Port Oper Priority        | Priority value assigned to this aggregation port by the partner.                          |
| Admin Key                 | Current administrative value of the Key for the protocol partner.                         |
| Oper Key                  | Current operational value of the Key for the protocol partner.                            |
| Admin State               | Administrative values of the partner's state parameters. (See preceding table.)           |
| Oper State                | Operational values of the partner's state parameters. (See preceding table.)              |

```

Console#show lacp sysid
Port Channel      System Priority      System MAC Address
-----
                1                32768      00-30-F1-8F-2C-A7
                2                32768      00-30-F1-8F-2C-A7
                3                32768      00-30-F1-8F-2C-A7
                4                32768      00-30-F1-8F-2C-A7
                5                32768      00-30-F1-8F-2C-A7
                6                32768      00-30-F1-8F-2C-A7
                7                32768      00-30-F1-D4-73-A0
                8                32768      00-30-F1-D4-73-A0
                9                32768      00-30-F1-D4-73-A0
               10                32768      00-30-F1-D4-73-A0
               11                32768      00-30-F1-D4-73-A0
               12                32768      00-30-F1-D4-73-A0
               :

```

**Table 78: show lacp sysid - display description**

| Field               | Description   |
|---------------------|---|
| Channel group       | A link aggregation group configured on this switch. |
| System Priority*    | LACP system priority for this channel group.        |
| System MAC Address* | System MAC address.                                 |

\* 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#
```

## 13

# 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 79: Port Mirroring Commands**

| Command              | Function  |
|----------------------|---|
| Local Port Mirroring | Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port |
| RSPAN Mirroring      | Mirrors data from remote switches over a dedicated VLAN   |

## Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

**Table 80: Mirror Port Commands**

| Command           | Function                                  | Mode |
|-------------------|---|------|
| port monitor      | Configures a mirror session               | IC   |
| show port monitor | Shows the configuration for a mirror port | PE   |

**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: 1-12)

**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 xxxxxxxxxxxx.

*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.
- ◆ All VLAN mirror sessions must share the same target port, preferably one that is not a member of the source VLAN.
- ◆ 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.
- ◆ Spanning Tree BPDU packets are not mirrored to the target port.

- ◆ 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.
- ◆ You can create multiple mirror sessions, but all sessions must share the same destination port.
- ◆ The destination port cannot be a trunk or trunk member port.
- ◆ 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 5:

```
Console(config)#interface ethernet 1/5
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:

```
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: 1-12)

*vlan-id* - VLAN ID (Range: 1-4094)

*mac-address* - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

### 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 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination Port (listen port):Eth1/5
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 81: RSPAN Commands

| Command                        | Function  | Mode |
|--------------------------------|---|------|
| <code>vlan rspan</code>        | Creates a VLAN dedicated to carrying RSPAN traffic  | VC   |
| <code>rspan source</code>      | Specifies the source port and traffic type to be mirrored   | GC   |
| <code>rspan destination</code> | Specifies the destination port to monitor the mirrored traffic                                    | GC   |
| <code>rspan remote vlan</code> | Specifies the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports | GC   |
| <code>no rspan session</code>  | Deletes a configured RSPAN session  | GC   |
| <code>show rspan</code>        | Displays the configuration settings for an RSPAN session  | PE   |

### 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 and switch cluster VLAN 4093 are 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: 1-12)

**rx** - Mirror received packets.

**tx** - Mirror transmitted packets.

**both** - Mirror both received and transmitted packets.

### Default Setting

Both TX and RX traffic is mirrored

### 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.
- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN source port – access ports are not allowed (see [switchport mode](#)).

- ◆ 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: 1-12)

**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  
Console(config)#
```

**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: 2-4094)

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: 1-12)

### 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 82: Congestion Control Commands**

| Command Group             | Function   |
|---------------------------|--|
| Rate Limiting             | Sets the input and output rate limits for a port.  |
| Storm Control             | Sets the traffic storm threshold for each port.  |
| Automatic Traffic Control | Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port. |

## 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 83: Rate Limit Commands**

| Command    | Function   | Mode |
|------------|--|------|
| rate-limit | Configures the maximum input or output rate for an interface | IC   |

**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 for Gigabit Ethernet ports)

### 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 84: Rate Limit Commands**

| Command                                 | Function   | Mode   |
|---|--|--------|
| storm-sample-type                       | Toggles threshold value units of storm control settings to be either packets per second or kilobits per second | GC     |
| <code>switchport packet-rate</code> *   | Configures broadcast, multicast, and unknown unicast storm control thresholds                                  | IC     |
| <code>show interfaces switchport</code> | Displays the administrative and operational status of an interface   | NE, PE |

\* 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; i.e., kilobits per second (kbps).  
(Range: 64-1000000 for Gigabit Ethernet ports)

### Default Setting

Broadcast Storm Control: Enabled, packet-rate limit: 64 kbps

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.



**Note:** Due to a chip limitation, this switch shares a common storm control threshold for unknown unicast, broadcast, and multicast traffic. The last storm control threshold set will be applied to all of these traffic types.

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

### 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 85: ATC Commands**

| Command  | Function  | Mode |
|--|---|------|
| <i>Threshold Commands</i>                        |   |      |
| <a href="#">auto-traffic-control apply-timer</a> | Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold | GC   |

Table 85: ATC Commands (Continued)

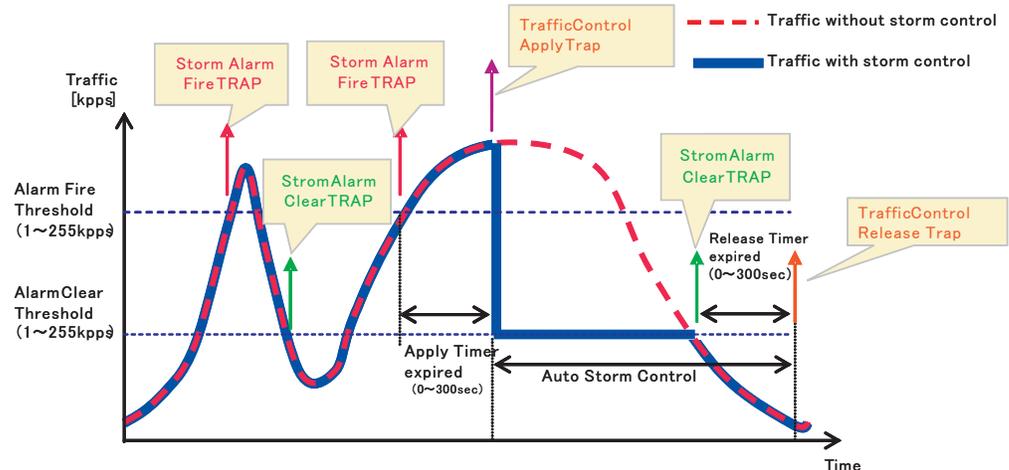
| Command  | Function  | Mode      |
|--|---|-----------|
| <code>auto-traffic-control release-timer</code>                          | Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold                                   | GC        |
| <code>auto-traffic-control*</code>                                       | Enables automatic traffic control for broadcast or multicast storms   | IC (Port) |
| <code>auto-traffic-control action</code>                                 | Sets the control action to limit ingress traffic or shut down the offending port  | IC (Port) |
| <code>auto-traffic-control alarm-clear-threshold</code>                  | Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent   | IC (Port) |
| <code>auto-traffic-control alarm-fire-threshold</code>                   | Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires                         | IC (Port) |
| <code>auto-traffic-control auto-control-release</code>                   | Automatically releases a control response   | IC (Port) |
| <code>auto-traffic-control control-release</code>                        | Manually releases a control response  | PE        |
| <i>SNMP Trap Commands</i>  |   |           |
| <code>snmp-server enable port-traps atc broadcast-alarm-clear</code>     | Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered                               | IC (Port) |
| <code>snmp-server enable port-traps atc broadcast-alarm-fire</code>      | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control   | IC (Port) |
| <code>snmp-server enable port-traps atc broadcast-control-apply</code>   | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires                               | IC (Port) |
| <code>snmp-server enable port-traps atc broadcast-control-release</code> | 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) |
| <code>snmp-server enable port-traps atc multicast-alarm-clear</code>     | Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered                               | IC (Port) |
| <code>snmp-server enable port-traps atc multicast-alarm-fire</code>      | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control   | IC (Port) |
| <code>snmp-server enable port-traps atc multicast-control-apply</code>   | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires                               | IC (Port) |
| <code>snmp-server enable port-traps atc multicast-control-release</code> | 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) |
| <i>ATC Display Commands</i>  |   |           |
| <code>show auto-traffic-control</code>                                   | Shows global configuration settings for automatic storm control   | PE        |
| <code>show auto-traffic-control interface</code>                         | 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.

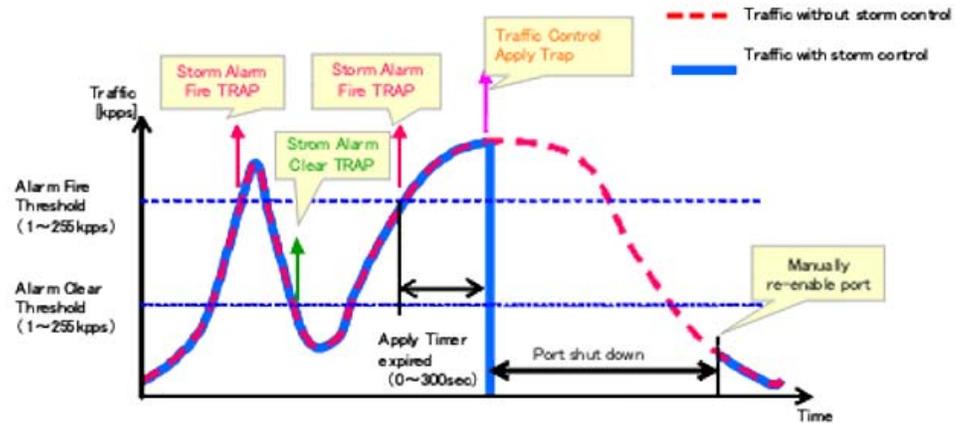
Figure 1: Storm Control by Limiting the Traffic Rate



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: 1-300 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: 1-900 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.

**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.

```
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

**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)

### Default Setting

128 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

128 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: 1-12)

#### 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#(config-if)
```

## 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

```
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 \(435\)](#)

[auto-traffic-control alarm-clear-threshold \(436\)](#)

**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

```
Console#auto-traffic-control broadcast control-release interface ethernet 1/1  
Console(config-if)#
```

### Related Commands

[auto-traffic-control alarm-fire-threshold \(437\)](#)

**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 \(437\)](#)

[auto-traffic-control apply-timer \(433\)](#)

#### **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 \(436\)](#)

[auto-traffic-control action \(435\)](#)

[auto-traffic-control release-timer \(434\)](#)

#### **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

### Command Mode

Interface Configuration (Ethernet)

### Example

```
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 \(435\)](#)

[auto-traffic-control alarm-clear-threshold \(436\)](#)

**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(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 \(437\)](#)

**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 \(437\)](#)  
[auto-traffic-control apply-timer \(433\)](#)

**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 \(436\)](#)  
[auto-traffic-control action \(435\)](#)  
[auto-traffic-control release-timer \(434\)](#)

## 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
```

```
release-timer (sec) : 900

Storm-control: Multicast
Apply-timer(sec)    : 300
release-timer(sec)  : 900
Console#
```

**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: 1-12)

### 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): 128          128
Alarm Clear Threshold(Kpps):128          128
Trap Storm Fire:        Disabled          Disabled
Trap Storm Clear:       Disabled          Disabled
Trap Traffic Apply:     Disabled          Disabled
Trap Traffic Release:   Disabled          Disabled

Console#
```

# UniDirectional Link Detection Commands

The switch can be configured to detect and disable unidirectional Ethernet fiber or copper links. When enabled, the protocol advertises a port's identity and learns about its neighbors on a specific LAN segment; and stores information about its neighbors in a cache. It can also send out a train of echo messages under circumstances that require fast notifications or re-synchronization of the cached information.

**Table 86: UniDirectional Link Detection Commands**

| Command                              | Function   | Mode |
|--------------------------------------|--|------|
| <code>udld detection-interval</code> | Sets the amount of time the switch remains in detection state after discovering a neighbor                                       | GC   |
| <code>udld message-interval</code>   | Configures the message interval between UDLD probe messages  | GC   |
| <code>udld recovery</code>           | Automatically recovers from UDLD disabled port state after a period specified by the <code>udld recovery-interval</code> command | GC   |
| <code>udld recovery-interval</code>  | Specifies the period after which to automatically recover from UDLD disabled port state  | GC   |
| <code>udld aggressive</code>         | Sets UDLD to aggressive mode on an interface   | IC   |
| <code>udld port</code>               | Enables UDLD on a port   | IC   |
| <code>show udld</code>               | Shows UDLD configuration settings and operational status   | PE   |

**udld detection-interval** This command sets the amount of time the switch remains in detection state after discovering a neighbor. Use the **no** form to restore the default setting.

## Syntax

**udld detection-interval** *detection-interval*

**no detection-interval**

*detection-interval* – The amount of time the switch remains in detection state after discovering a neighbor through UDLD. (Range: 5-255 seconds)

## Default Setting

5 seconds

## Command Mode

Global Configuration

### Command Usage

When a neighbor device is discovered by UDLD, the switch enters “detection state” and remains in this state for specified detection-interval. After the detection-interval expires, the switch tries to decide whether or the link is unidirectional based on the information collected during “detection state.”

### Example

```
Console(config)#udld detection-interval 10
Console(config)#
```

**udld message-interval** This command configures the message interval between UDLD probe messages for ports in the advertisement phase and determined to be bidirectional. Use the **no** form to restore the default setting.

### Syntax

**udld message-interval** *message-interval*

**no message-interval**

*message-interval* – The interval at which a port sends UDLD probe messages after linkup or detection phases. (Range: 7-90 seconds)

### Default Setting

15 seconds

### Command Mode

Global Configuration

### Command Usage

During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171.

If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds).

If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.

### Example

This example sets the message interval to 10 seconds.

```
Console(config)#udld message-interval 10
Console(config)#
```

**udld recovery** This command configures the switch to automatically recover from UDLD disabled port state after a period specified by the [udld recovery-interval](#) command. Use the **no** form to disable this feature.

#### Syntax

**[no] udld recovery**

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Command Usage

When automatic recovery state is changed by this command, any ports shut down by UDLD will be reset.

#### Example

```
Console(config)#udld recovery
Console(config)#
```

**udld recovery-interval** This command specifies the period after which to automatically recover from UDLD disabled port state. Use the **no** form to restore the default setting.

**udld recovery-interval** *recovery-interval*

**no recovery-interval**

*recovery-interval* – The interval after which a port is reset after being placed in UDLD disabled state. (Range: 30-86400 seconds)

#### Default Setting

7 seconds

#### Command Mode

Global Configuration

#### Command Usage

- ◆ This command is only applicable when automatic recovery has been enabled with the [udld recovery](#) command.
- ◆ When the recovery interval is changed by this command, any ports shut down by UDLD will be reset.

### Example

```
Console(config)#udld recovery-interval 15
Console(config)#
```

**udld aggressive** This command sets UDLD to aggressive mode on an interface. Use the **no** form to restore the default setting.

### Syntax

**[no] udld aggressive**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet Port)

### Command Usage

UDLD can function in two modes: normal mode and aggressive mode.

- ◆ In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that's information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are "event-based." If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach to minimize false positives during the detection process and deems a port to be in "undetermined" state. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.
- ◆ In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).

### Example

This example enables UDLD aggressive mode on port 1.

```

Console(config)#interface ethernet 1/1
Console(config-if)#udld aggressive
Console(config-if)#

```

**udld port** This command enables UDLD on a port. Use the **no** form to disable UDLD on an interface.

### Syntax

**[no] udld port**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet Port)

### Command Usage

- ◆ UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential mis-configuration to be detected and for prompt corrective action to be taken.
- ◆ Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.)

Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is considered to be unidirectional.

### Example

```

Console(config)#interface ethernet 1/1
Console(config-if)#udld port
Console(config-if)#

```

**show udd** This command shows UDLD configuration settings and operational status for the switch or for a specified interface.

**Syntax**

**show udd** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**Command Mode**

Privileged Exec

**Example**

```

Console#show udd
Message Interval : 15
Detection Interval : 5 seconds
Recovery : Disabled
Recovery Interval : 300 seconds

Interface UDLD Mode Oper State Msg Invl
Port State Det Invl
-----
Eth 1/ 1 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 2 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 3 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 4 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 5 Disabled Normal Disabled 7 s
Unknown 5 s
:
Console#show udd interface ethernet 1/1
Interface UDLD Mode Oper State Msg Invl
Port State Det Invl
-----
Eth 1/ 1 Disabled Normal Disabled 7 s
Unknown 5 s

Console#
    
```

**Table 87: show udd - display description**

| Field              | Description   |
|--------------------|---|
| Message Interval   | The interval between UDLD probe messages for ports in advertisement phase     |
| Detection Interval | The period the switch remains in detection state after discovering a neighbor |
| Recovery           | Shows if automatic recovery from UDLD disabled port state is enabled          |

**Table 87: show uddl - display description** (Continued)

| Field             | Description   |
|-------------------|---|
| Recovery Interval | Shows the period after which to recover from UDLD disabled port state if automatic recovery is enabled  |
| UDLD              | Shows if UDLD is enabled or disabled on a port  |
| Mode              | Shows if UDLD is functioning in Normal or Aggressive mode   |
| Oper State        | Shows the UDLD operational state (Disabled, Link down, Link up, Advertisement, Detection, Disabled port, Advertisement - Single neighbor, Advertisement - Multiple neighbors)   |
| Port State        | Shows the UDLD port state (Unknown, Bidirectional, Unidirectional, Transmit-to-receive loop, Mismatch with neighbor state reported, Neighbor's echo is empty)<br>The state is Unknown if the link is down or not connected to a UDLD-capable device. The state is Bidirectional if the link has a normal two-way connection to a UDLD-capable device. All other states indicate mis-wiring. |
| Msg Invl          | The interval between UDLD probe messages used for the indicated operational state   |
| Det Invl          | The period the switch remains in detection state after discovering a neighbor   |
| Timeout           | The time that UDLD waits for echoes from a neighbor device during the detection window  |



# 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 88: Address Table Commands**

| Command  | Function   | Mode |
|--|--|------|
| <code>mac-address-table aging-time</code>      | Sets the aging time of the address table   | GC   |
| <code>mac-address-table static</code>          | Maps a static address to a port in a VLAN  | GC   |
| <code>clear mac-address-table dynamic</code>   | Removes any learned entries from the forwarding database                         | PE   |
| <code>show mac-address-table</code>            | Displays entries in the bridge-forwarding database                               | PE   |
| <code>show mac-address-table aging-time</code> | Shows the aging time for the address table                                       | PE   |
| <code>show mac-address-table count</code>      | Shows the number of MAC addresses used and the number of available MAC addresses | PE   |

**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*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*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

### Command Usage

Even if a hash collision for a MAC address is resolved, entries in the collision MAC address table are not removed until this command is issued to reset the table, or the system is reset.

### 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*]  
[**vlan** *vlan-id*]  
[**sort** {**address** | **vlan** | **interface**}]

*mac-address* - MAC address.

*mask* - Bits to match in the address.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*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
  - Security - Port Security
- ◆ 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      70-72-CF-59-8F-40          1 CPU      Delete on Reset
Eth 1/ 1 00-60-61-B1-84-4A    1 Learn     Delete on Timeout
Eth 1/ 0 00-E0-0C-10-90-00    1 Learn     Delete on Timeout
Eth 1/ 1 00-E0-0C-10-90-0E    1 Learn     Delete on Timeout
Eth 1/ 1 00-E0-4C-68-12-66    1 Learn     Delete on Timeout
Eth 1/ 1 CC-37-AB-7F-AF-C0    1 Learn     Delete on Timeout
Eth 1/ 1 CC-37-AB-BB-DE-60    1 Learn     Delete on Timeout

Console#

```

**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.
Console#

```

**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*

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

#### 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      :3
Static Address Count     :0
Dynamic Address Count    :3
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 89: Spanning Tree Commands**

| Command   | Function  | Mode |
|---|---|------|
| <code>spanning-tree</code>                      | Enables the spanning tree protocol  | GC   |
| <code>spanning-tree cisco-prestandard</code>    | Configures spanning tree operation to be compatible with Cisco prestandard versions                               | GC   |
| <code>spanning-tree forward-time</code>         | Configures the spanning tree bridge forward time  | GC   |
| <code>spanning-tree hello-time</code>           | Configures the spanning tree bridge hello time  | GC   |
| <code>spanning-tree max-age</code>              | Configures the spanning tree bridge maximum age   | GC   |
| <code>spanning-tree mode</code>                 | Configures STP, RSTP or MSTP mode   | GC   |
| <code>spanning-tree pathcost method</code>      | Configures the path cost method for RSTP/MSTP   | GC   |
| <code>spanning-tree priority</code>             | Configures the spanning tree bridge priority  | GC   |
| <code>spanning-tree mst configuration</code>    | Changes to MSTP configuration mode  | GC   |
| <code>spanning-tree system-bpdu-flooding</code> | Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled | GC   |
| <code>spanning-tree transmission-limit</code>   | Configures the transmission limit for RSTP/MSTP   | GC   |
| <code>max-hops</code>                           | Configures the maximum number of hops allowed in the region before a BPDU is discarded                            | MST  |
| <code>mst priority</code>                       | Configures the priority of a spanning tree instance   | MST  |
| <code>mst vlan</code>                           | Adds VLANs to a spanning tree instance  | MST  |
| <code>name</code>                               | Configures the name for the multiple spanning tree  | MST  |
| <code>revision</code>                           | Configures the revision number for the multiple spanning tree   | MST  |
| <code>spanning-tree bpdu-filter</code>          | Filters BPDUs for edge ports  | IC   |
| <code>spanning-tree bpdu-guard</code>           | Shuts down an edge port if it receives a BPDU   | IC   |
| <code>spanning-tree cost</code>                 | Configures the spanning tree path cost of an interface  | IC   |
| <code>spanning-tree edge-port</code>            | Enables fast forwarding for edge ports  | IC   |
| <code>spanning-tree link-type</code>            | Configures the link type for RSTP/MSTP  | IC   |
| <code>spanning-tree loopback-detection</code>   | Enables BPDU loopback detection for a port  | IC   |

Table 89: Spanning Tree Commands (Continued)

| Command  | Function  | Mode |
|--|---|------|
| <code>spanning-tree loopback-detection action</code>       | Configures the response for loopback detection to block user traffic or shut down the interface   | IC   |
| <code>spanning-tree loopback-detection release-mode</code> | Configures loopback release mode for a port   | IC   |
| <code>spanning-tree loopback-detection trap</code>         | Enables BPDU loopback SNMP trap notification for a port   | IC   |
| <code>spanning-tree mst cost</code>                        | Configures the path cost of an instance in the MST  | IC   |
| <code>spanning-tree mst port-priority</code>               | Configures the priority of an instance in the MST   | IC   |
| <code>spanning-tree port-bpdu-flooding</code>              | Floods BPDUs to other ports when global spanning tree is disabled   | IC   |
| <code>spanning-tree port-priority</code>                   | Configures the spanning tree priority of an interface   | IC   |
| <code>spanning-tree root-guard</code>                      | Prevents a designated port from passing superior BPDUs  | IC   |
| <code>spanning-tree spanning-disabled</code>               | Disables spanning tree for an interface   | IC   |
| <code>spanning-tree loopback-detection release</code>      | Manually releases a port placed in discarding state by loopback-detection   | PE   |
| <code>spanning-tree protocol-migration</code>              | Re-checks the appropriate BPDU format   | PE   |
| <code>show spanning-tree</code>                            | Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree | PE   |
| <code>show spanning-tree mst configuration</code>          | Shows the multiple spanning tree configuration  | PE   |

**spanning-tree** 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 setting.

### 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  $[(\text{max-age} / 2) + 1]$ .

### 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 \(461\)](#)

[spanning-tree max-age \(463\)](#)

**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 x (hello-time + 1)].

The maximum value is the lower of 40 or [2 x (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 \(461\)](#)

[spanning-tree hello-time \(462\)](#)

**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

rstp

### 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 473](#)) takes precedence over port priority ([page 481](#)).
- ◆ 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 40000
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 \(469\)](#)

[mst priority \(469\)](#)

[name \(470\)](#)

revision (471)  
max-hops (468)

**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 32 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 470](#)) 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 471](#)) 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 \(471\)](#)

**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 470](#)) 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 \(470\)](#)

**spanning-tree bpd-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 bpd-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.
- ◆ BPDU filter can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto 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 \(474\)](#)

**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 BPDUs. 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.
- ◆ BPDU guard can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto 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-guard
Console(config-if)#
```

### Related Commands

[spanning-tree edge-port \(474\)](#)

[spanning-tree spanning-disabled \(483\)](#)

**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)<sup>9</sup>

**Table 90: Recommended STA Path Cost Range**

| Port Type        | Short Path Cost<br>(IEEE 802.1D-1998) | Long Path Cost<br>(IEEE 802.1D-2004) |
|------------------|---------------------------------------|--------------------------------------|
| Ethernet         | 50-600                                | 200,000-20,000,000                   |
| Fast Ethernet    | 10-60                                 | 20,000-2,000,000                     |
| Gigabit Ethernet | 3-10                                  | 2,000-200,000                        |

### 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

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).

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 91: Default STA Path Costs**

| Port Type        | Short Path Cost (IEEE 802.1D-1998) | Long Path Cost (IEEE 802.1D-2004) |
|------------------|------------------------------------|-----------------------------------|
| Ethernet         | 65,535                             | 1,000,000                         |
| Fast Ethernet    | 65,535                             | 100,000                           |
| Gigabit Ethernet | 10,000                             | 10,000                            |

### 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.
- ◆ When the path cost method ([page 465](#)) 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.
- ◆ When edge port is set as auto, the operational state is determined automatically by the Bridge Detection State Machine described in 802.1D-2004, where the edge port state may change dynamically based on environment changes (e.g., receiving a BPDU or not within the required interval).

### 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 BPDUs 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
```

### spanning-tree loopback-detection action

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

{**block** | **shutdown** *duration*}

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

### 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

**auto** - Allows a port to automatically be released from the discarding state when the loopback state ends.

**manual** - The port can only be released from the discarding state manually.

**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 its own, or;
  - The port's link status changes to link down and then link up again, or;
  - The port ceases to receive its own BPDUs in a forward delay interval.
- ◆ 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.
- ◆ 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** *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<sup>10</sup>, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in [Table 90 on page 473](#).

### 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 in [Table 91](#). 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 91 on page 474](#).

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Each spanning-tree instance is associated with a unique set of VLAN IDs.
- ◆ 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.

<sup>10</sup>. Use the [spanning-tree pathcost method](#) command to set the path cost method.

### 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 \(480\)](#)

**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 \(479\)](#)

**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 \(473\)](#)

**spanning-tree root-guard** This command prevents a designated port<sup>11</sup> 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.

11. See Port Role under "Displaying Interface Settings for STA" in the *Web Management Guide*.

- ◆ 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(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(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*instance-id* - Instance identifier of the multiple spanning tree.  
(Range: 0-4094)

**brief** - Shows a summary of global and interface settings.

**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** command to display the spanning tree configuration for all instances within the Multiple Spanning Tree (MST), including global settings and settings for active interfaces.
- ◆ 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
External Admin Path Cost     : 0
Internal Admin Path Cost     : 0
External Oper Path Cost      : 100000
Internal Oper Path Cost      : 100000
Priority                      : 128
Designated Cost              : 100000
Designated Port              : 128.1
Designated Root              : 32768.0.0001ECF8D8C6
Designated Bridge            : 32768.0.123412341234
Forward Transitions          : 4
Admin Edge Port              : Disabled
Oper Edge Port               : Disabled
Admin Link Type              : Auto
Oper Link Type               : Point-to-point
Flooding Behavior            : Enabled
Spanning-Tree Status        : Enabled
Loopback Detection Status    : Enabled
Loopback Detection Release Mode : Auto
Loopback Detection Trap      : Disabled
Loopback Detection Action    : Block
Root Guard Status           : Disabled
BPDU Guard Status           : Disabled
BPDU Guard Auto Recovery    : Disabled
BPDU Guard Auto Recovery Interval : 300
BPDU Filter Status          : Disabled
.
.
.

```

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              : 32768.0000E89382A0
Current Root Port            : 0
Current Root Cost             : 0

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#

```



# ERPS Commands

The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings.

This chapter describes commands used to configure ERPS.

**Table 92: ERPS Commands**

| Command                           | Function   | Mode |
|-----------------------------------|--|------|
| <code>erps</code>                 | Enables ERPS globally on the switch  | GC   |
| <code>erps domain</code>          | Creates an ERPS ring and enters ERPS configuration mode  | GC   |
| <code>control-vlan</code>         | Adds a Control VLAN to an ERPS ring  | ERPS |
| <code>enable</code>               | Activates the current ERPS ring  | ERPS |
| <code>guard-timer</code>          | Sets the timer to prevent ring nodes from receiving outdated R-APS messages                                    | ERPS |
| <code>holdoff-timer</code>        | Sets the timer to filter out intermittent link faults  | ERPS |
| <code>major-domain</code>         | Specifies the ERPS ring used for sending control packets   | ERPS |
| <code>meg-level</code>            | Sets the Maintenance Entity Group level for a ring   | ERPS |
| <code>mep-monitor</code>          | Specifies the CCM MEPs used to monitor the link on a ring node   | ERPS |
| <code>node-id</code>              | Sets the MAC address for a ring node   | ERPS |
| <code>non-erps-dev-protect</code> | Sends non-standard health-check packets when in protection state   | ERPS |
| <code>non-revertive</code>        | Enables non-revertive mode, which requires the protection state on the RPL to manually cleared                 | ERPS |
| <code>propagate-tc</code>         | Enables propagation of topology change messages from a secondary ring to the primary ring                      | ERPS |
| <code>raps-def-mac</code>         | Sets the switch's MAC address to be used as the node identifier in R-APS messages                              | ERPS |
| <code>raps-without-vc</code>      | Terminates the R-APS channel at the primary ring to sub-ring interconnection nodes                             | ERPS |
| <code>ring-port</code>            | Configures a node's connection to the ring through the east or west interface                                  | ERPS |
| <code>rpl neighbor</code>         | Configures a ring node to be the RPL neighbor  | ERPS |
| <code>rpl owner</code>            | Configures a ring node to be the RPL owner   | ERPS |
| <code>version</code>              | Specifies compatibility with ERPS version 1 or 2   | ERPS |
| <code>wtr-timer</code>            | Sets timer to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure | ERPS |

Table 92: ERPS Commands (Continued)

| Command                            | Function   | Mode |
|------------------------------------|--|------|
| <code>clear erps statistics</code> | Clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages  | PE   |
| <code>erps clear</code>            | Manually clears protection state which has been invoked by a Forced Switch or Manual Switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode | PE   |
| <code>erps forced-switch</code>    | Blocks the specified ring port   | PE   |
| <code>erps manual-switch</code>    | Blocks the specified ring port, in the absence of a failure or an erps forced-switch command   | PE   |
| <code>show erps</code>             | Displays status information for all configured rings, or for a specified ring  | PE   |

### Configuration Guidelines for ERPS

1. Create an ERPS ring: Create a ring using the `erps domain` command. The ring name is used as an index in the G.8032 database.
2. Configure the east and west interfaces: Each node on the ring connects to it through two ring ports. Use the `ring-port` command to configure one port connected to the next node in the ring to the east (or clockwise direction); and then use the `ring-port` command again to configure another port facing west in the ring.
3. Configure the RPL owner: Configure one node in the ring as the Ring Protection Link (RPL) owner using the `rpl owner` command. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL. Under normal operations (Idle state), the RPL is blocked to ensure that a loop cannot form in the ring. If a signal failure brings down any other link in the ring, the RPL will be unblocked (Protection state) to ensure proper connectivity among all ring nodes until the failure is recovered.
4. Configure ERPS timers: Use the `guard-timer` command to set the timer is used to prevent ring nodes from receiving outdated R-APS messages, the `holdoff-timer` command to filter out intermittent link faults, and the `wtr-timer` command to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.
5. Configure the ERPS Control VLAN (CVLAN): Use the `control-vlan` command to create the VLAN used to pass R-APS ring maintenance commands. The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN (prior to configuring the VLAN as a CVLAN). No other ports can be members of this VLAN (once set as a CVLAN). Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

6. Enable ERPS: Before enabling a ring as described in the next step, first use the `erps` command to globally enable ERPS on the switch. If ERPS has not yet been enabled or has been disabled with the `no erps` command, no ERPS rings will work.
7. Enable an ERPS ring: Before an ERPS ring can work, it must be enabled using the `enable` command. When configuration is completed and the ring enabled, R-APS messages will start flowing in the control VLAN, and normal traffic will begin to flow in the data VLANs. To stop a ring, it can be disabled on any node using the `no enable` command.
8. Display ERPS status information: Use the `show erps` command to display general ERPS status information or detailed ERPS status information for a specific ring.

**erps** This command enables ERPS on the switch. Use the **no** form to disable this feature.

### Syntax

**[no] erps**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

ERPS must be enabled globally on the switch before it can be enabled on an ERPS ring using the `enable` command.

### Example

```
Console(config)#erps
Console(config)#
```

### Related Commands

[enable \(493\)](#)

**erps domain** This command creates an ERPS ring and enters ERPS configuration mode for the specified domain. Use the **no** form to delete a ring.

### Syntax

**erps domain** *ring-name* [**id** *ring-id*]

**no erps domain** *ring-name*

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

*ring-id* - ERPS ring identifier used in R-APS messages. (Range: 1-255)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

- ◆ Service Instances within each ring are based on a unique maintenance association for the specific users, distinguished by the ring name, maintenance level, maintenance association's name, and assigned VLAN. Up to 6 ERPS rings can be configured on the switch.
- ◆ R-APS information is carried in an R-APS PDUs. The last octet of the MAC address is designated as the Ring ID (01-19-A7-00-00-[Ring ID]). If use of the default MAC address is disabled with the `no raps-def-mac` command, then the Ring ID configured by the **erps domain** command will be used in R-APS PDUs.

### Example

```
Console(config)#erps domain r&d id 1
Console(config-erps)#
```

**control-vlan** This command specifies a dedicated VLAN used for sending and receiving ERPS protocol messages. Use the **no** form to remove the Control VLAN.

### Syntax

**[no] control-vlan** *vlan-id*

*vlan-id* - VLAN ID (Range: 1-4094)

### Default Setting

None

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN ([vlan, page 528](#)), add the ring ports for the east and west interface as tagged members to this VLAN ([switchport allowed vlan, page 531](#)), and then use the `control-vlan` command to add it to the ring.

- ◆ The following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:
  - The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.
  - In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.
  - Also, the ring ports of the Control VLAN must be tagged.
- ◆ Once the ring has been activated with the `enable` command, the configuration of the control VLAN cannot be modified. Use the `no enable` command to stop the ERPS ring before making any configuration changes to the control VLAN.

### Example

```

Console(config)#vlan database
Console(config-vlan)#vlan 2 name rdc media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#interface ethernet 1/11
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#exit
Console(config)#erps domain rd1
Console(config-erps)#control-vlan 2
Console(config-erps)#

```

**enable** This command activates the current ERPS ring. Use the **no** form to disable the current ring.

### Syntax

**[no] enable**

### Default Setting

Disabled

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Before enabling a ring, the global ERPS function should be enabled with the `erps` command, the east and west ring ports configured on each node with the `ring-port` command, the RPL owner specified with the `rpl owner` command, and the control VLAN configured with the `control-vlan` command.
- ◆ Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

**Example**

```
Console(config-erps)#enable
Console(config-erps)#
```

**Related Commands**[erps \(491\)](#)

**guard-timer** This command sets the guard timer to prevent ring nodes from receiving outdated R-APS messages. Use the **no** form to restore the default setting.

**Syntax**

**guard-timer** *milliseconds*

*milliseconds* - The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds)

**Default Setting**

500 milliseconds

**Command Mode**

ERPS Configuration

**Command Usage**

The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

**Example**

```
Console(config-erps)#guard-timer 300
Console(config-erps)#
```

**holdoff-timer** This command sets the timer to filter out intermittent link faults. Use the **no** form to restore the default setting.

**Syntax**

**holdoff-timer** *milliseconds*

*milliseconds* - The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds)

**Default Setting**

0 milliseconds

**Command Mode**

ERPS Configuration

**Command Usage**

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer.

When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

**Example**

```
Console(config-erps)#holdoff-timer 300
Console(config-erps)#
```

**major-domain** This command specifies the ERPS ring used for sending control packets. Use the **no** form to remove the current setting.

**Syntax**

**major-domain** *name*

**no major-domain**

*name* - Name of the ERPS ring used for sending control packets.  
(Range: 1-32 characters)

**Default Setting**

None

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ This switch can support up to six rings. However, ERPS control packets can only be sent on one ring. This command is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets.
- ◆ The Ring Protection Link (RPL) is the west port and can not be configured. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a

secondary ring (or sub-domain) which can have only one physical ring port. This command will therefore fail if the east port is already configured (see the [ring-port](#) command).

### Example

```
Console(config-erps)#major-domain rd0
Console(config-erps)#
```

**meg-level** This command sets the Maintenance Entity Group level for a ring. Use the **no** form to restore the default setting.

### Syntax

**meg-level** *level*

*level* - The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7)

### Default Setting

1

### Command Mode

ERPS Configuration

### Command Usage

- ◆ This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.
- ◆ If CFM continuity check messages are used to monitor the link status of an ERPS ring node as specified by the [mep-monitor](#) command, then the MEG level set by the **meg-level** command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs. The MEP's primary VLAN must also be the same as that used for the ERPS ring's control VLAN.

### Example

```
Console(config-erps)#meg-level 0
Console(config-erps)#
```

### Related Commands

[ethernet cfm domain \(741\)](#)

[ethernet cfm mep \(746\)](#)

**mep-monitor** This command specifies the CFM MEPs used to monitor the link on a ring node. Use the **no** form to restore the default setting.

### Syntax

**mep-monitor** {**east** | **west**} **mep** *mpid*

**east** - Connects to next ring node to the east.

**west** - Connects to next ring node to the west.

*mpid* – Maintenance end point identifier. (Range: 1-8191)

### Default Setting

None

### Command Mode

ERPS Configuration

### Command Usage

- ◆ If this command is used to monitor the link status of an ERPS node with CFM continuity check messages, then the MEG level set by the [meg-level](#) command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs.
- ◆ To ensure complete monitoring of a ring node, use the **mep-monitor** command to specify the CFM MEPs used to monitor both the east and west ports of the ring node.
- ◆ If CFM determines that a MEP node which has been configured to monitor a ring port with this command has gone down, this information is passed to ERPS, which in turn processes it as a ring node failure. For more information on how ERPS recovers from a node failure, refer to “Ethernet Ring Protection Switching” in the *Web Management Guide*.

### Example

```
Console(config-erps)#mep-monitor east mep 1
Console(config-erps)#
```

**Related Commands**[ethernet cfm domain \(741\)](#)[ethernet cfm mep \(746\)](#)

**node-id** This command sets the MAC address for a ring node. Use the **no** form to restore the default setting.

**Syntax**

**node-id** *mac-address*

*mac-address* – A MAC address unique to the ring node. The MAC address must be specified in the format *xx-xx-xx-xx-xx-xx* or *xxxxxxxxxxxx*.

**Default Setting**

CPU MAC address

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ The ring node identifier is used to identify a node in R-APS messages for both automatic and manual switching recovery operations.

For example, a node that has one ring port in SF condition and detects that the condition has been cleared, will continuously transmit R-APS (NR) messages with its own Node ID as priority information over both ring ports, informing its neighbors that no request is present at this node. When another recovered node holding the link blocked receives this message, it compares the Node ID information with its own. If the received R-APS (NR) message has a higher priority, this unblocks its ring ports. Otherwise, the block remains unchanged.

- ◆ The node identifier may also be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

**Example**

```
Console(config-erps)#node-id 00-12-CF-61-24-2D
Console(config-erps)#
```

**non-erps-dev-protect** This command sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through SF messages. Use the **no** form to disable this feature.

### Syntax

**[no] non-erps-dev-protect**

### Default Setting

Disabled

### Command Mode

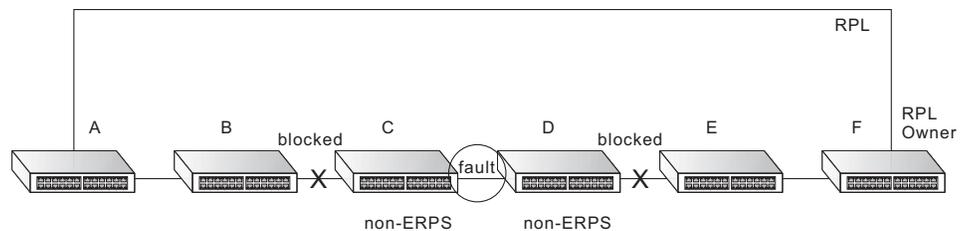
ERPS Configuration

### Command Usage

- ◆ The RPL owner node detects a failed link when it receives R-APS (SF - signal fault) messages from nodes adjacent to the failed link. The owner then enters protection state by unblocking the RPL. However, using this standard recovery procedure may cause a non-ERPS device to become isolated when the ERPS device adjacent to it detects a continuity check message (CCM) loss event and blocks the link between the non-ERPS device and ERPS device.

CCMs are propagated by the Connectivity Fault Management (CFM) protocol as described under [“CFM Commands” on page 735](#). If the standard recovery procedure were used as shown in the following figure, and node E detected CCM loss, it would send an R-APS (SF) message to the RPL owner and block the link to node D, isolating that non-ERPS device.

**Figure 3: Non-ERPS Device Protection**



When non-ERPS device protection is enabled on the ring, the ring ports on the RPL owner node and non-owner nodes will not be blocked when signal loss is detected by CCM loss events.

- ◆ When non-ERPS device protection is enabled on an RPL owner node, it will send non-standard health-check packets to poll the ring health when it enters the protection state. It does not use the normal procedure of waiting to receive an R-APS (NR - no request) message from nodes adjacent to the recovered link. Instead, it waits to see if the non-standard health-check packets loop back. If they do, indicating that the fault has been resolved, the RPL will be blocked.

After blocking the RPL, the owner node will still transmit an R-APS (NR, RB - ring blocked) message. ERPS-compliant nodes receiving this message flush their

forwarding database and unblock previously blocked ports. The ring is now returned to Idle state.

### Example

```
Console(config-erps)#non-erps-dev-protect
Console(config-erps)#
```

**non-revertive** This command enables non-revertive mode, which requires the protection state on the RPL to manually cleared. Use the **no** form to restore the default revertive mode.

### Syntax

**[no] non-revertive**

### Default Setting

Disabled

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Revertive behavior allows the switch to automatically return the RPL from Protection state to Idle state through the exchange of protocol messages.

Non-revertive behavior for Protection, Forced Switch, and Manual Switch states are basically the same. Non-revertive behavior requires the [erps clear](#) command to used to return the RPL from Protection state to Idle state.

- ◆ Recovery for Protection Switching – A ring node that has one or more ring ports in an SF (Signal Fail) condition, upon detecting the SF condition cleared, keeps at least one of its ring ports blocked for the traffic channel and for the R-APS channel, until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

A ring node that has one ring port in an SF condition and detects the SF condition cleared, continuously transmits the R-APS (NR – no request) message with its own Node ID as the priority information over both ring ports, informing that no request is present at this ring node and initiates a guard timer. When another recovered ring node (or nodes) holding the link block receives this message, it compares the Node ID information with its own Node ID. If the received R-APS (NR) message has the higher priority, this ring node unblocks its ring ports. Otherwise, the block remains unchanged. As a result, there is only one link with one end blocked.

The ring nodes stop transmitting R-APS (NR) messages when they accept an R-APS (NR, RB – RPL Blocked), or when another higher priority request is received.



is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

If the ring node where the Forced Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message over both ring ports.

- Recovery with revertive mode is handled in the following way:
  - a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTB timer.
  - b. The WTB timer is cancelled if during the WTB period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.
  - c. When the WTB timer expires, in the absence of any other higher priority request, the RPL Owner Node initiates reversion by blocking the traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes the FDB.
  - d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.
  
- Recovery with non-revertive mode is handled in the following way:
  - a. The RPL Owner Node, upon reception of an R-APS(NR) message and in the absence of any other higher priority request does not perform any action.
  - b. Then, after the operator issues the `erps clear` command at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message on both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.
  - c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.
  
- ◆ Recovery for Manual Switching – An `erps manual-switch` command is removed by issuing the `erps clear` command at the same ring node where the Manual Switch is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

The ring node where the Manual Switch was cleared keeps the ring port blocked for the traffic channel and for the R-APS channel, due to the previous Manual Switch command. This ring port is kept blocked until the RPL is blocked

as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

The Ethernet Ring Node where the Manual Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

If the ring node where the Manual Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message on both ring ports.

- Recovery with revertive mode is handled in the following way:
  - a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request, starts the WTB timer and waits for it to expire. While the WTB timer is running, any latent R-APS (MS) message is ignored due to the higher priority of the WTB running signal.
  - b. When the WTB timer expires, it generates the WTB expire signal. The RPL Owner Node, upon reception of this signal, initiates reversion by blocking the traffic channel on the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.
  - c. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all Ethernet Ring Nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.
  
- Recovery with non-revertive mode is handled in the following way:
  - a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request does not perform any action.
  - b. Then, after the operator issues the `erps clear` command at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.
  - c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.

**Example**

```
Console(config-erps) #non-revertive
Console(config-erps) #
```

**propagate-tc** This command enables propagation of topology change messages for a secondary ring to the primary ring. Use the **no** form to disable this feature.

**Syntax**

**[no] propagate-tc**

**Default Setting**

Disabled

**Command Mode**

ERPS Configuration

**Command Usage**

- ◆ When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through protection switching.
- ◆ When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

**Example**

```
Console(config-erps) #propagate-tc
Console(config-erps) #
```

**raps-def-mac** This command sets the switch's MAC address to be used as the node identifier in R-APS messages. Use the **no** form to use the node identifier specified in the G8032 standards.

**Syntax**

**[no] raps-def-mac**

**Default Setting**

Enabled

### Command Mode

ERPS Configuration

### Command Usage

- ◆ When ring nodes running ERPSv1 and ERPSv2 co-exist on the same ring, the Ring ID of each ring node must be configured as “1”.
- ◆ If this command is disabled, the following strings are used as the node identifier:
  - ERPSv1: 01-19-A7-00-00-01
  - ERPSv2: 01-19-A7-00-00-[Ring ID]

### Example

```
Console(config-erps)#raps-def-mac
Console(config-erps)#
```

**raps-without-vc** This command terminates the R-APS channel at the primary ring to sub-ring interconnection nodes. Use the **no** form to restore the default setting.

### Syntax

**[no] raps-without-vc**

### Default Setting

R-APS with Virtual Channel

### Command Mode

ERPS Configuration

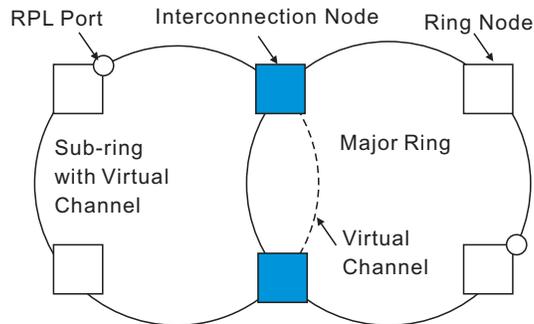
### Command Usage

- ◆ A sub-ring may be attached to a primary ring with or without a virtual channel. A virtual channel is used to connect two interconnection points on the sub-ring, tunneling R-APS control messages across an arbitrary Ethernet network topology. If a virtual channel is not used to cross the intermediate Ethernet network, data in the traffic channel will still flow across the network, but the all R-APS messages will be terminated at the interconnection points.
- ◆ Sub-ring with R-APS Virtual Channel – When using a virtual channel to tunnel R-APS messages between interconnection points on a sub-ring, the R-APS virtual channel may or may not follow the same path as the traffic channel over the network. R-APS messages that are forwarded over the sub-ring’s virtual channel are broadcast or multicast over the interconnected network. For this reason the broadcast/multicast domain of the virtual channel should be limited to the necessary links and nodes. For example, the virtual channel could span only the interconnecting rings or sub-rings that are necessary for forwarding R-APS messages of this sub-ring. Care must also be taken to ensure that the local RAPS messages of the sub-ring being transported over the virtual channel

into the interconnected network can be uniquely distinguished from those of other interconnected ring R-APS messages. This can be achieved by, for example, by using separate VIDs for the virtual channels of different sub-rings.

Note that the R-APS virtual channel requires a certain amount of bandwidth to forward R-APS messages on the interconnected Ethernet network where a sub-ring is attached. Also note that the protection switching time of the sub-ring may be affected if R-APS messages traverse a long distance over an R-APS virtual channel.

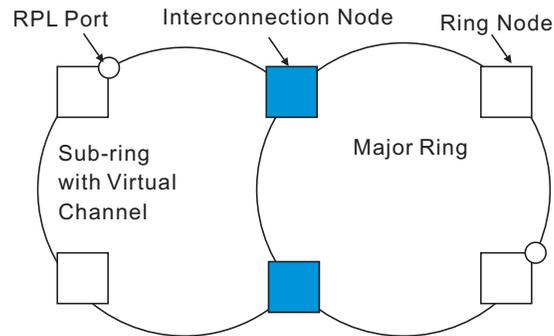
**Figure 4: Sub-ring with Virtual Channel**



- ◆ **Sub-ring without R-APS Virtual Channel** – Under certain circumstances it may not be desirable to use a virtual channel to interconnect the sub-ring over an arbitrary Ethernet network. In this situation, the R-APS messages are terminated on the interconnection points. Since the sub-ring does not provide an R-APS channel nor R-APS virtual channel beyond the interconnection points, R-APS channel blocking is not employed on the normal ring links to avoid channel segmentation. As a result, a failure at any ring link in the sub-ring will cause the R-APS channel of the sub-ring to be segmented, thus preventing R-APS message exchange between some of the sub-ring's ring nodes.

No R-APS messages are inserted or extracted by other rings or sub-rings at the interconnection nodes where a sub-ring is attached. Hence there is no need for either additional bandwidth or for different VIDs/Ring IDs for the ring interconnection. Furthermore, protection switching time for a sub-ring is independent from the configuration or topology of the interconnected rings. In addition, this option always ensures that an interconnected network forms a tree topology regardless of its interconnection configuration. This means that it is not necessary to take precautions against forming a loop which is potentially composed of a whole interconnected network.

Figure 5: Sub-ring without Virtual Channel



### Example

```
Console(config-erps) #raps-without-vc
Console(config-erps) #
```

**ring-port** This command configures a node's connection to the ring through the east or west interface. Use the **no** form to disassociate a node from the ring.

### Syntax

**ring-port** {east | west} interface *interface*

**east** - Connects to next ring node to the east.

**west** - Connects to next ring node to the west.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### Default Setting

Not associated

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction.
- ◆ Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk.

- ◆ If a port channel (static trunk) is specified as a ring port, it can not be destroyed before it is removed from the domain configuration.
- ◆ A static trunk will be treated as a signal fault, if it contains no member ports or all of its member ports are in signal fault.
- ◆ If a static trunk is configured as a ring port prior to assigning any member ports, spanning tree will be disabled for the first member port assigned to the static trunk.

### Example

```
Console(config-erps)#ring-port east interface ethernet 1/12
Console(config-erps)#
```

**rpl neighbor** This command configures a ring node to be the Ring Protection Link (RPL) neighbor. Use the **no** form to restore the default setting.

### Syntax

```
rpl neighbor
no rpl
```

### Default Setting

None (that is, neither owner nor neighbor)

### Command Mode

ERPS Configuration

### Command Usage

- ◆ The RPL neighbor node, when configured, is a ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block at the other end by the RPL Owner Node. The RPL neighbor node may participate in blocking or unblocking its end of the RPL, but is not responsible for activating the reversion behavior.
- ◆ Only one RPL owner can be configured on a ring. If the switch is set as the RPL owner for an ERPS domain, the west ring port is set as one end of the RPL. If the switch is set as the RPL neighbor for an ERPS domain, the east ring port is set as the other end of the RPL.
- ◆ The east and west connections to the ring must be specified for all ring nodes using the [ring-port](#) command. When this switch is configured as the RPL neighbor, the east ring port is set as being connected to the RPL.
- ◆ Note that is not mandatory to declare a RPL neighbor.

### Example

```
Console(config-erps)#rpl neighbor
Console(config-erps)#
```

**rpl owner** This command configures a ring node to be the Ring Protection Link (RPL) owner. Use the **no** form to restore the default setting.

### Syntax

**rpl owner**

**no rpl**

### Default Setting

None (that is, neither owner nor neighbor)

### Command Mode

ERPS Configuration

### Command Usage

- ◆ Only one RPL owner can be configured on a ring. The owner blocks traffic on the RPL during Idle state, and unblocks it during Protection state (that is, when a signal fault is detected on the ring or the protection state is enabled with the [erps forced-switch](#) or [erps manual-switch](#) command).
- ◆ The east and west connections to the ring must be specified for all ring nodes using the [ring-port](#) command. When this switch is configured as the RPL owner, the west ring port is automatically set as being connected to the RPL.

### Example

```
Console(config-erps)#rpl owner
Console(config-erps)#
```

**version** This command specifies compatibility with ERPS version 1 or 2.

### Syntax

**version {1 | 2}**

1 - ERPS version 1 based on ITU-T G.8032/Y.1344.

2 - ERPS version 2 based on ITU-T G.8032/Y.1344 Version 2.

### Default Setting

2

## Command Mode

ERPS Configuration

## Command Usage

- ◆ In addition to the basic features provided by version 1, version 2 also supports:
  - Multi-ring/ladder network support
  - Revertive/Non-revertive recovery
  - Forced Switch (FS) and Manual Switch (MS) commands for manually blocking a particular ring port
  - Flush FDB (forwarding database) logic which reduces amount of flush FDB operations in the ring
  - Support of multiple ERP instances on a single ring
- ◆ Version 2 is backward compatible with Version 1. If version 2 is specified, the inputs and commands are forwarded transparently. If set to version 1, MS and FS operator commands are filtered, and the switch set to revertive mode.
- ◆ The version number is automatically set to "1" when a ring node, supporting only the functionalities of G.8032v1, exists on the same ring with other nodes that support G.8032v2.
- ◆ When ring nodes running G.8032v1 and G.8032v2 co-exist on a ring, the ring ID of each node is configured as "1".
- ◆ In version 1, the MAC address 01-19-A7-00-00-01 is used for the node identifier. The `raps-def-mac` command has no effect.

## Example

```

Console(config-erps)#version 1
Console(config-erps)#

```

**wtr-timer** This command sets the wait-to-restore timer which is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. Use the **no** form to restore the default setting.

## Syntax

**wtr-timer** *minutes*

*minutes* - The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes)

## Default Setting

5 minutes

**Command Mode**

ERPS Configuration

**Command Usage**

If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

**Example**

```
Console(config-erps)#wtr-timer 10
Console(config-erps)#
```

**clear erps statistics** This command clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages.

**Syntax**

**clear erps statistics** [**domain** *ring-name*]

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

**Command Mode**

Privileged Exec

**Example**

```
Console#clear erps statistics domain r&d
Console#
```

**erps clear** This command manually clears the protection state which has been invoked by a forced switch or manual switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode.

**Syntax**

**erps clear domain** *ring-name*

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

**Command Mode**

Privileged Exec

**Command Usage**

- ◆ Two steps are required to make a ring operating in non-revertive mode return to Idle state from forced switch or manual switch state:
  1. Issue an **erps clear** command to remove the forced switch command on the node where a local forced switch command is active.
  2. Issue an **erps clear** command on the RPL owner node to trigger the reversion.
- ◆ The **erps clear** command will also stop the WTR and WTB delay timers and reset their values.
- ◆ More detailed information about using this command for non-revertive mode is included under the Command Usage section for the [non-revertive](#) command.

**Example**

```
Console#erps clear domain r&d
Console#
```

**erps forced-switch** This command blocks the specified ring port.

**Syntax**

**erps forced-switch** [**domain** *ring-name*] {**east** | **west**}

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

**east** - East ring port.

**west** - West ring port.

**Command Mode**

Privileged Exec

**Command Usage**

- ◆ A ring with no pending request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the **erps forced-switch** command triggers protection switching as follows:
  - a. The ring node where a forced switch command was issued blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.
  - b. The ring node where the forced switch command was issued transmits R-APS messages indicating FS over both ring ports. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command (see [Table 93 on page 513](#)). The

R-APS (FS) message informs other ring nodes of the FS command and that the traffic channel is blocked on one ring port.

- c. A ring node accepting an R-APS (FS) message, without any local higher priority requests unblocks any blocked ring port. This action subsequently unblocks the traffic channel over the RPL.
  - d. The ring node accepting an R-APS (FS) message, without any local higher priority requests stops transmission of R-APS messages.
  - e. The ring node receiving an R-APS (FS) message flushes its FDB.
- ◆ Protection switching on a forced switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on the following rules apply regarding processing of further forced switch commands:

While an existing forced switch request is present in a ring, any new forced switch request is accepted, except on a ring node having a prior local forced switch request. The ring nodes where further forced switch commands are issued block the traffic channel and R-APS channel on the ring port at which the forced switch was issued. The ring node where the forced switch command was issued transmits an R-APS message over both ring ports indicating FS. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command. As such, two or more forced switches are allowed in the ring, which may inadvertently cause the segmentation of an ring. It is the responsibility of the operator to prevent this effect if it is undesirable.

Ring protection requests, commands and R-APS signals have the priorities as specified in the following table.

**Table 93: ERPS Request/State Priority**

| Request / State and Status | Type   | Priority |
|----------------------------|--------|----------|
| Clear                      | local  | highest  |
| FS                         | local  |          |
| R-APS (FS)                 | remote |          |
| local SF*                  | local  |          |
| local clear SF             | local  |          |
| R-APS (SF)                 | remote |          |
| R-APS (MS)                 | remote |          |
| MS                         | local  |          |
| WTR Expires                | local  |          |
| WTR Running                | local  |          |
| WTB Expires                | local  |          |

**Table 93: ERPS Request/State Priority** (Continued)

| Request / State and Status | Type   | Priority |
|----------------------------|--------|----------|
| WTB Running                | local  |          |
| R-APS (NR, RB)             | remote |          |
| R-APS (NR)                 | remote | lowest   |

\* If an Ethernet Ring Node is in the Forced Switch state, local SF is ignored.

- ◆ Recovery for forced switching under revertive and non-revertive mode is described under the Command Usage section for the [non-revertive](#) command.
- ◆ When a ring is under an FS condition, and the node at which an FS command was issued is removed or fails, the ring remains in FS state because the FS command can only be cleared at node where the FS command was issued. This results in an unrecoverable FS condition.

When performing a maintenance procedure (e.g., replacing, upgrading) on a ring node (or a ring link), it is recommended that FS commands be issued at the two adjacent ring nodes instead of directly issuing a FS command at the ring node under maintenance in order to avoid falling into the above mentioned unrecoverable situation.

### Example

```
Console#erps forced-switch domain r&d west
Console#
```

**erps manual-switch** This command blocks the specified ring port, in the absence of a failure or an [erps forced-switch](#) command.

### Syntax

**erps manual-switch** [**domain** *ring-name*] {**east** | **west**}

*ring-name* - Name of a specific ERPS ring. (Range: 1-12 characters)

**east** - East ring port.

**west** - West ring port.

### Command Mode

Privileged Exec

### Command Usage

- ◆ A ring with no request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the **erps manual-switch** command triggers protection switching as follows:
  - a. If no other higher priority commands exist, the ring node, where a manual switch command was issued, blocks the traffic channel and R-APS channel

on the ring port to which the command was issued, and unblocks the other ring port.

- b.** If no other higher priority commands exist, the ring node where the manual switch command was issued transmits R-APS messages over both ring ports indicating MS. R-APS (MS) messages are continuously transmitted by this ring node while the local MS command is the ring node's highest priority command (see [Table 93 on page 513](#)). The R-APS (MS) message informs other ring nodes of the MS command and that the traffic channel is blocked on one ring port.
  - c.** If no other higher priority commands exist and assuming the ring node was in Idle state before the manual switch command was issued, the ring node flushes its local FDB.
  - d.** A ring node accepting an R-APS (MS) message, without any local higher priority requests unblocks any blocked ring port which does not have an SF condition. This action subsequently unblocks the traffic channel over the RPL.
  - e.** A ring node accepting an R-APS (MS) message, without any local higher priority requests stops transmitting R-APS messages.
  - f.** A ring node receiving an R-APS (MS) message flushes its FDB.
- ◆ Protection switching on a manual switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on, the following rules apply regarding processing of further manual switch commands:
    - a.** While an existing manual switch request is present in the ring, any new manual switch request is rejected. The request is rejected at the ring node where the new request is issued and a notification is generated to inform the operator that the new MS request was not accepted.
    - b.** A ring node with a local manual switch command which receives an R-APS (MS) message with a different Node ID clears its manual switch request and starts transmitting R-APS (NR) messages. The ring node keeps the ring port blocked due to the previous manual switch command.
    - c.** An ring node with a local manual switch command that receives an R-APS message or a local request of higher priority than R-APS (MS) clear its manual switch request. The ring node then processes the new higher priority request.
  - ◆ Recovery for manual switching under revertive and non-revertive mode is described under the Command Usage section for the [non-revertive](#) command.

**Example**

```
Console#erps manual-switch domain r&d west
Console#
```

**show erps** This command displays status information for all configured rings, or for a specified ring

**Syntax**

**show erps** [**domain** *ring-name*] [**statistics**]

**domain** - Keyword to display ERPS ring configuration settings.

*ring-name* - Name of a specific ERPS ring. (Range: 1-32 characters)

**statistics** - Keyword to display ERPS ring statistics.

**Command Mode**

Privileged Exec

**Example**

This example displays a summary of all the ERPS rings configured on the switch.

```
Console#show erps
ERPS Status           : Enabled
Number of ERPS Domains : 1

Domain      ID  Enabled Ver  MEL Ctrl VLAN State      Type      Revertive
-----
r&d         1  Yes    2    1      1 Idle    RPL Owner  Yes

           W/E  Interface Port State Local SF Local FS Local MS MEP  RPL
-----
West Eth 1/ 1  Blocking No      No      No      No      Yes
East Eth 1/ 3  Forwarding No      No      No      No      No

Console#
```

**Table 94: show erps - summary display description**

| Field                   | Description   |
|-------------------------|---|
| <i>Node Information</i> |   |
| ERPS Status             | Shows whether ERPS is enabled on the switch.                                  |
| Number of ERPS Domains  | Shows the number of ERPS rings configured on the switch.                      |
| Domain                  | Displays the name of each ring followed by a brief list of status information |
| ID                      | ERPS ring identifier used in R-APS messages.                                  |
| Enabled                 | Shows if the specified ring is enabled.                                       |
| Ver                     | Shows the ERPS version.   |

**Table 94: show erps - summary display description** (Continued)

| Field                        | Description  |
|------------------------------|--|
| MEL                          | The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.  |
| Ctrl VLAN                    | Shows the Control VLAN ID.   |
| State                        | Shows the following ERPS states:<br><br>Init – The ERPS ring has started but has not yet determined the status of the ring.<br><br>Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs.<br><br>Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.   |
| Type                         | Shows ERPS node type as None, RPL Owner or RPL Neighbor.   |
| Revertive                    | Shows if revertive or non-revertive recovery is selected.  |
| <i>Interface Information</i> |  |
| W/E                          | Shows information on the west and east ring port for this node.  |
| Interface                    | The port or trunk which is configured as a ring port.  |
| Port State                   | The operational state:<br><br>Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.<br><br>Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed.<br><br>Unknown – The interface is not in a known state (includes the domain being disabled). |
| Local SF                     | A signal fault generated on a link to the local node.  |
| Local FS                     | Shows if a forced switch command was issued on this interface.   |
| Local MS                     | Shows if a manual switch command was issued on this interface.   |
| MEP                          | The CFM MEP used to monitor the status on this link.   |
| RPL                          | Shows if this node is connected to the RPL.  |

This example displays detailed information for the specified ERPS ring.

```

Console#show erps domain rd1
Domain      ID  Enabled Ver  MEL  Ctrl  VLAN  State      Type      Revertive
-----
r&d        1  Yes      2    1      1  Idle      RPL Owner  Yes

          Major Domain Node ID          R-APS With VC
          -----
          00-E0-0C-00-00-FD Yes

R-APS Def MAC Propagate TC Non-ERPS Device Protect
-----
Yes          No          No

```

```

Holdoff  Guard  WTB      WTR      WTB Expire WTR Expire
-----  -----  -----  -----  -----  -----
      0 ms  500 ms 5500 ms   5 min

W/E  Interface  Port  State  Local  SF  Local  FS  Local  MS  MEP  RPL
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
West Eth 1/ 1  Blocking  No      No      No      No
East Eth 1/ 3  Forwarding No      No      No      No
    
```

Console#

Table 94 on page 516 describes most of the parameters shown by **show erps domain** command. The following table includes the remaining parameters.

**Table 95: show erps domain - detailed display description**

| Field                   | Description  |
|-------------------------|--|
| Major Domain            | Name of the ERPS major domain.   |
| Node ID                 | A MAC address unique to this ring node.  |
| R-APS with VC           | The R-APS Virtual Channel is the R-APS channel connection used to tunnel R-APS messages between two interconnection nodes of a sub-ring in another Ethernet ring or network.             |
| R-APS Def MAC           | Indicates if the switch's MAC address is used to identify the node in R-APS messages.  |
| Propagate TC            | Shows if the ring is configured to propagate topology change notification messages.  |
| Non-ERPS Device Protect | Shows if the RPL owner node is configured to send non-standard health-check packets when it enters protection state without any link down event having been detected through SF messages |
| Holdoff                 | The hold-off timer interval used to filter out intermittent link faults.   |
| Guard                   | The guard timer interval used to prevent ring nodes from receiving outdated R-APS messages.  |
| WTB                     | The wait-to-block timer interval used to delay reversion after a Forced Switch or Manual Switch has been cleared.  |
| WTR                     | The wait-to-restore timer interval used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.   |
| WTB Expire              | The time before the wait-to-block timer expires.   |
| WTR Expire              | The time before the wait-to-restore timer expires.   |

This example displays statistics for all configured ERPS rings.

```

Console#show erps statistics
ERPS statistics for domain r&d :
Interface  Local SF  Local Clear SF
-----  -----  -----
(W) Eth 1/ 1  0          0
              SF          NR          NR-RB        FS          MS
-----  -----  -----  -----  -----  -----
Sent              0          62          948          0          0
Received          0          0           0           0          0
Ignored           0          0           0           0          0
    
```

```

          EVENT      HEALTH
          -----
Sent          0          0
Received      0          0
Ignored       0          0

Interface    Local SF    Local Clear SF
-----
(E) Eth 1/ 3 0          0
          SF          NR          NR-RB          FS          MS
-----
Sent          0          62          948          0          0
Received      0          0          0          0          0
Ignored       0          0          0          0          0
          EVENT      HEALTH
          -----
Sent          0          0
Received      0          0
Ignored       0          0
Console#

```

**Table 96: show erps statistics - detailed display description**

| Field          | Description   |
|----------------|---|
| Interface      | The direction, and port or trunk which is configured as a ring port.  |
| Local SF       | A signal fault generated on a link to the local node.   |
| Local Clear SF | The number of times a clear command was issued to terminate protection state entered through a forced switch or manual switch |
| SF             | The number of signal fault messages   |
| NR             | The number of no request messages   |
| NR-RB          | The number no request - RPL blocked messages  |
| FS             | The number of forced switch messages  |
| MS             | The number of manual switch messages  |
| EVENT          | Any request/state message, excluding FS, SF, MS, and NR   |
| HEALTH         | The number of non-standard health-check messages  |



# VLAN Commands

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 97: VLAN Commands**

| Command Group  | Function  |
|--|---|
| <a href="#">GVRP and Bridge Extension Commands</a>           | Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB                                |
| <a href="#">Editing VLAN Groups</a>                          | Sets up VLAN groups, including name, VID and state  |
| <a href="#">Configuring VLAN Interfaces</a>                  | Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP                            |
| <a href="#">Displaying VLAN Information</a>                  | Displays VLAN groups, status, port members, and MAC addresses   |
| <a href="#">Configuring IEEE 802.1Q Tunneling</a>            | Configures 802.1Q Tunneling (QinQ Tunneling)  |
| <a href="#">Configuring L2PT Tunneling<sup>1</sup></a>       | Configures Layer 2 Protocol Tunneling (L2PT), either by discarding, processing, or transparently passing control packets across a QinQ tunnel |
| <a href="#">Configuring VLAN Translation<sup>1</sup></a>     | Maps VLAN ID between customer and service provider for networks that do not support IEEE 802.1Q tunneling                                     |
| <a href="#">Configuring Protocol-based VLANs<sup>2</sup></a> | Configures protocol-based VLANs based on frame type and protocol  |
| <a href="#">Configuring IP Subnet VLANs<sup>2</sup></a>      | Configures IP Subnet-based VLANs  |
| <a href="#">Configuring MAC Based VLANs<sup>2</sup></a>      | Configures MAC-based VLANs  |
| <a href="#">Configuring Voice VLANs</a>                      | Configures VoIP traffic detection and enables a Voice VLAN  |

1 These functions are not compatible.

2 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 98: GVRP and Bridge Extension Commands**

| Command                                | Function   | Mode   |
|--|--|--------|
| <code>bridge-ext gvrp</code>           | Enables GVRP globally for the switch                   | GC     |
| <code>garp timer</code>                | Sets the GARP timer for the selected function          | IC     |
| <code>switchport forbidden vlan</code> | Configures forbidden VLANs for an interface            | IC     |
| <code>switchport gvrp</code>           | Enables GVRP for an interface                          | IC     |
| <code>show bridge-ext</code>           | Shows the global bridge extension configuration        | PE     |
| <code>show garp timer</code>           | Shows the GARP timer for the selected function         | NE, PE |
| <code>show gvrp configuration</code>   | Displays GVRP configuration for the selected interface | NE, PE |

**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 \(526\)](#)

**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).
- ◆ This command will not be accepted if the specified VLAN does not exist on the switch.

### 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
Console#
```

**show garp timer** This command shows the GARP timers for the selected interface.

### Syntax

**show garp timer** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### Default Setting

Shows all GARP timers.

### Command Mode

Normal Exec, Privileged Exec

### Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
Join Timer      : 20 centiseconds
Leave Timer     : 60 centiseconds
Leave All Timer : 1000 centiseconds
Console#
```

### Related Commands

[garp timer \(523\)](#)

**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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 99: Commands for Editing VLAN Groups**

| Command                       | Function   | Mode |
|-------------------------------|--|------|
| <a href="#">vlan database</a> | Enters VLAN database mode to add, change, and delete VLANs | GC   |
| <a href="#">vlan</a>          | Configures a VLAN, including VID, name and state           | VC   |

**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 \(536\)](#)

**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 420](#).

### 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 \(536\)](#)

## Configuring VLAN Interfaces

Table 100: Commands for Configuring VLAN Interfaces

| Command   | Function   | Mode |
|---|--|------|
| <a href="#">interface vlan</a>                    | Enters interface configuration mode for a specified VLAN | IC   |
| <a href="#">switchport acceptable-frame-types</a> | Configures frame types to be accepted by an interface    | IC   |
| <a href="#">switchport allowed vlan</a>           | Configures the VLANs associated with an interface        | IC   |
| <a href="#">switchport forbidden vlan</a>         | Configures forbidden VLANs for an interface              | IC   |
| <a href="#">switchport gvrp</a>                   | Enables GVRP for an interface                            | IC   |
| <a href="#">switchport ingress-filtering</a>      | Enables ingress filtering on an interface                | IC   |
| <a href="#">switchport mode</a>                   | Configures VLAN membership mode for an interface         | IC   |
| <a href="#">switchport native vlan</a>            | Configures the PVID (native VLAN) of an interface        | IC   |
| <a href="#">switchport priority default</a>       | Sets a port priority for incoming untagged frames        | IC   |
| <a href="#">vlan-trunking</a>                     | Allows unknown VLANs to cross the switch                 | IC   |

**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 \(377\)](#)

[interface \(370\)](#)

[vlan \(528\)](#)

### 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 \(533\)](#)

**switchport allowed vlan** This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

### Syntax

```
switchport allowed vlan {add vlan-list [tagged | untagged] |  
remove vlan-list}
```

#### **no switchport allowed vlan**

**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.

*vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4093). 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).

### 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 \(530\)](#)

**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)#
```

**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

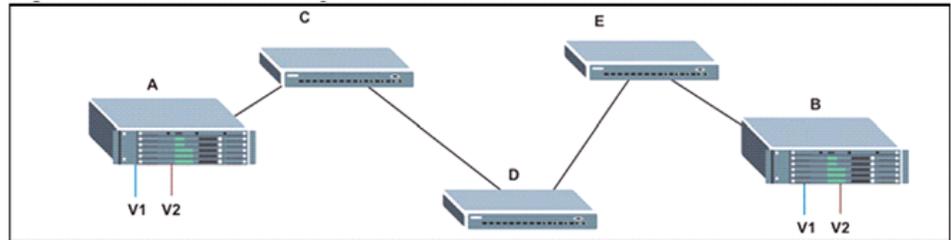
Interface Configuration (Ethernet, Port Channel)

#### 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.

Figure 6: Configuring VLAN Trunking



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 9 and 10 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/9
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/10
Console(config-if)#vlan-trunking
Console(config-if)#
```

## Displaying VLAN Information

This section describes commands used to display VLAN information.

**Table 101: Commands for Displaying VLAN Information**

| Command                                  | Function   | Mode   |
|--|--|--------|
| <code>show interfaces status vlan</code> | Displays status for the specified VLAN interface                   | NE, PE |
| <code>show interfaces switchport</code>  | Displays the administrative and operational status of an interface | NE, PE |
| <code>show vlan</code>                   | Shows VLAN information   | NE, PE |

**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)

Console#
```

## Configuring IEEE 802.1Q Tunneling

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 102: 802.1Q Tunneling Commands**

| Command   | Function   | Mode |
|---|--|------|
| <code>dot1q-tunnel system-tunnel-control</code>         | Configures the switch to operate in normal mode or QinQ mode   | GC   |
| <code>switchport dot1q-tunnel mode</code>               | Configures an interface as a QinQ tunnel port                  | IC   |
| <code>switchport dot1q-tunnel service match cvid</code> | Creates a CVLAN to SPVLAN mapping entry                        | IC   |
| <code>switchport dot1q-tunnel tpid</code>               | Sets the Tag Protocol Identifier (TPID) value of a tunnel port | IC   |
| <code>show dot1q-tunnel</code>                          | Displays the configuration of QinQ tunnel ports                | PE   |
| <code>show interfaces switchport</code>                 | Displays port QinQ operational status                          | PE   |

### *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 `switchport 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 \(543\)](#)

[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 \(543\)](#)

[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.

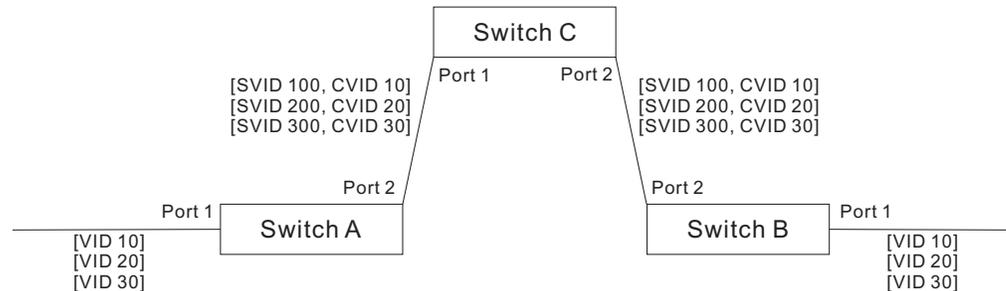
#### Example

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 7: 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. Configures 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. Configures 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
```

| Port     | Match | C-VID | S-VID |
|----------|-------|-------|-------|
| Eth 1/ 1 |       | 10    | 100   |
| Eth 1/ 1 |       | 20    | 200   |
| Eth 1/ 1 |       | 30    | 300   |

## 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
```

**switchport dot1q-tunnel tpid** This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

### Syntax

**switchport dot1q-tunnel tpid** *tpid*

**no switchport 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

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. 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 only applies to ports configured in Uplink mode using the **switchport dot1q-tunnel mode** command. If the port is in normal mode (i.e., unspecified), the TPID is always 8100. If the port is in Access mode, received packets are processed as untagged packets.

### Example

```
Console(config)#interface ethernet 1/1  
Console(config-if)#switchport dot1q-tunnel tpid 9100  
Console(config-if)#
```

## Related Commands

[show interfaces switchport \(389\)](#)

**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* - Stack unit. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*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

Port      Mode    TPID (hex)
-----
Eth 1/ 1 Access      8100
Eth 1/ 2 Uplink      8100
Eth 1/ 3 Normal      8100
:
:
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

Port      Match C-VID S-VID
-----
Eth 1/ 5          1  100
Eth 1/ 6          1  100

Console#

```

**Related Commands**  
[switchport dot1q-tunnel mode \(539\)](#)

## Configuring L2PT Tunneling

This section describes the commands used to configure Layer 2 Protocol Tunneling (L2PT).

**Table 103: L2 Protocol Tunnel Commands**

| Command                                       | Function  | Mode |
|---|---|------|
| <a href="#">l2protocol-tunnel tunnel-dmac</a> | Configures the destination address for Layer 2 Protocol Tunneling | GC   |
| <a href="#">switchport l2protocol-tunnel</a>  | Enables Layer 2 Protocol Tunneling for the specified protocol     | IC   |
| <a href="#">show l2protocol-tunnel</a>        | Shows settings for Layer 2 Protocol Tunneling                     | PE   |

**[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`.

The tunnel address can be any multicast address, except for the following:

- IPv4 multicast addresses (with prefix 01-00-5E)
- IPv6 multicast addresses (with prefix 33-33-33)
- Addresses used by the spanning tree protocol.

### 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<sup>12</sup> 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.

---

12. 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 VLAN Translation

QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the switches directly connected to that device can be configured to swap the customer's VLAN ID with the service provider's VLAN ID for upstream traffic, or the service provider's VLAN ID with the customer's VLAN ID for downstream traffic.

This section describes commands used to configure VLAN translation.

**Table 104: VLAN Translation Commands**

| Command                                     | Function   | Mode |
|---|--|------|
| <a href="#">switchport vlan-translation</a> | Maps VLAN IDs between the customer and service provider  | IC   |
| <a href="#">show vlan-translation</a>       | Displays the configuration settings for VLAN translation | PE   |

**switchport vlan-translation** This command maps VLAN IDs between the customer and service provider.

#### Syntax

**switchport vlan-translation** *original-vlan new-vlan*

**no switchport vlan-translation** *original-vlan*

*original-vlan* - The original VLAN ID. (Range: 1-4094)

*new-vlan* - The new VLAN ID. (Range: 1-4094)

#### Default Setting

Disabled

## Command Mode

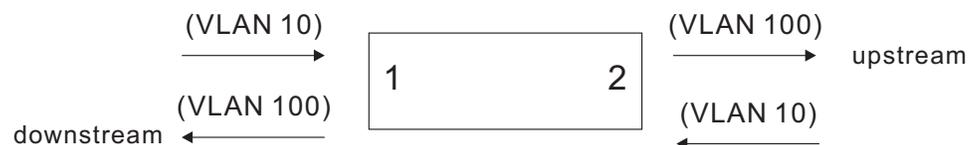
Interface Configuration (Ethernet)

## Command Usage

- ◆ If the next switch upstream does not support QinQ tunneling, then use this command to map the customer's VLAN ID to the service provider's VLAN ID for the upstream port. Similarly, if the next switch downstream does not support QinQ tunneling, then use this command to map the service provider's VLAN ID to the customer's VLAN ID for the downstream port. Note that one command maps both the *original-vlan* to *new-vlan* for ingress traffic and the *new-vlan* to *original-vlan* for egress traffic on the specified port.

For example, assume that the upstream switch does not support QinQ tunneling. If the command **switchport vlan-translation 10 100** is used to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1, then the VLAN IDs will be swapped as shown below.

Figure 8: Configuring VLAN Translation



- ◆ The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.
- ◆ If VLAN translation is set on an interface with this command, and the same interface is also configured as a QinQ access port with the **switchport dot1q-tunnel mode** command, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

## Example

This example configures VLAN translation for Port 1 as described in the Command Usage section above.

```
Console(config)#vlan database
Console(config-vlan)#vlan 10 media ethernet state active
Console(config-vlan)#vlan 100 media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/1,2
Console(config-if)#switchport allowed vlan add 10 tagged
Console(config-if)#switchport allowed vlan add 100 tagged
Console(config-if)#interface ethernet 1/1
Console(config-if)#switchport vlan-translation 10 100
Console(config-if)#end
Console#show vlan-translation
```

```
Interface Old VID New VID
-----
Eth 1/ 1      10    100

Console#
```

**show vlan-translation** This command displays the configuration settings for VLAN translation.

### Syntax

**show vlan-translation** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### Command Mode

Privileged Exec

### Example

```
Console#show vlan-translation

Interface Old VID New VID
-----
Eth 1/ 1      10    100

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 105: Protocol-based VLAN Commands**

| Command   | Function   | Mode |
|---|--|------|
| <code>protocol-vlan protocol-group</code>                 | Create a protocol group, specifying the supported protocols                | GC   |
| <code>protocol-vlan protocol-group</code>                 | Maps a protocol group to a VLAN  | IC   |
| <code>show protocol-vlan protocol-group</code>            | Shows the configuration of protocol groups                                 | PE   |
| <code>show interfaces protocol-vlan protocol-group</code> | Shows the interfaces mapped to a protocol group and the corresponding VLAN | PE   |

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 528). 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 add` command (Global Configuration mode).
3. Then map the protocol for each interface to the appropriate VLAN using the `protocol-vlan protocol-group vlan` command (Interface Configuration mode).



**Note:** Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN that has been configured with the switch's administrative IP interface (default VLAN 1). IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, network access can be regained by removing the offending Protocol VLAN rule via the console. Alternately, the switch can be power-cycled, however all unsaved configuration changes will be lost.

**protocol-vlan  
protocol-group**  
(Configuring Groups)

This command creates a protocol group, or adds 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*]

**no protocol-vlan protocol-group** *group-id*

*group-id* - Group identifier of this protocol group. (Range: 1-2147483647)

*frame*<sup>13</sup> - Frame type used by this protocol. (Options: ethernet, rfc\_1042, llc\_other)

*protocol* - Protocol type. The only option for the llc\_other frame type is ipx\_raw. The options for all other frames types include: arp, ip, ipv6, rarp.

**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  
Console(config)#
```

**protocol-vlan  
protocol-group**  
(Configuring Interfaces)

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)

13. SNAP frame types are not supported by this switch due to hardware limitations.

### 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 priority 0
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
          1 Ethernet    08 06
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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

## 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#show interfaces protocol-vlan protocol-group
PrPort Protocol Group ID VLAN ID Priority
-----
Eth 1/ 2 1                2      0
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 106: IP Subnet VLAN Commands**

| Command                                  | Function  | Mode |
|--|---|------|
| <code>subnet-vlan</code>                 | Defines the IP Subnet VLANs                         | GC   |
| <code>show interfaces subnet-vlan</code> | Displays a brief summary of IP Subnet VLAN settings | PE   |
| <code>show subnet-vlan</code>            | Displays IP Subnet VLAN settings                    | PE   |

**subnet-vlan** 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.

- ◆ 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 interfaces subnet-vlan

This command displays a brief summary of IP Subnet VLAN settings.

#### Syntax

**show interfaces subnet-vlan**

#### Command Mode

Privileged Exec

### Example

The following example displays a summary of configured IP subnet-based VLANs.

```
Console#show interfaces subnet-vlan
Port      IP Address      Mask
-----
Eth 1/1   192.168.12.0    255.255.255.128
Eth 1/2   192.168.12.128 255.255.255.192
Eth 1/3   192.168.12.192 255.255.255.224
Eth 1/4   192.168.12.224 255.255.255.240
Eth 1/5   192.168.12.240 255.255.255.248
Eth 1/6   192.168.12.248 255.255.255.252
Eth 1/7   192.168.12.252 255.255.255.254
Eth 1/8   192.168.12.254 255.255.255.255
Eth 1/9   192.168.12.255 255.255.255.255
Console#
```

**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 107: MAC Based VLAN Commands**

| Command       | Function                         | Mode |
|---------------|----------------------------------|------|
| mac-vlan      | Defines the IP Subnet VLANs      | GC   |
| show mac-vlan | Displays IP Subnet VLAN settings | PE   |

**mac-vlan** This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

### Syntax

**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**priority** *priority*]

**no mac-vlan mac-address** {*mac-address* | **all**}

*mac-address* – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format *xx-xx-xx-xx-xx-xx* or *xxxxxxxxxxxx*.

*vlan-id* – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4093)

*priority* – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

- ◆ The MAC-to-VLAN mapping applies to all ports on the switch.
- ◆ 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.

### 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)#
```

**show mac-vlan** This command displays MAC address-to-VLAN assignments.

### Command Mode

Privileged Exec

### Command Usage

Use this command to display MAC address-to-VLAN mappings.

### 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 108: Voice VLAN Commands**

| Command                                     | Function   | Mode |
|---|--|------|
| <code>voice vlan</code>                     | Defines the Voice VLAN ID                                  | GC   |
| <code>voice vlan aging</code>               | Configures the aging time for Voice VLAN ports             | GC   |
| <code>voice vlan mac-address</code>         | Configures VoIP device MAC addresses                       | GC   |
| <code>switchport voice vlan</code>          | Sets the Voice VLAN port mode                              | IC   |
| <code>switchport voice vlan priority</code> | Sets the VoIP traffic priority for ports                   | IC   |
| <code>switchport voice vlan rule</code>     | Sets the automatic VoIP traffic detection method for ports | IC   |
| <code>switchport voice vlan security</code> | Enables Voice VLAN security on ports                       | IC   |
| <code>show voice vlan</code>                | Displays Voice VLAN settings                               | PE   |

**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**

*minutes* - 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. (Range: 80-00-00-00-00-00 to FF-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 FF-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 711](#) 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                5 100
Eth 1/ 4 Auto      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-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

---

## Class of Service Commands

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 109: Priority Commands**

| Command Group                     | Function  |
|-----------------------------------|---|
| Priority Commands (Layer 2)       | Configures the queue mode, queue weights, and default priority for untagged frames  |
| Priority Commands (Layer 3 and 4) | 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 |

### Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

**Table 110: Priority Commands (Layer 2)**

| Command                                  | Function  | Mode |
|--|---|------|
| <code>queue mode</code>                  | Sets the queue mode to Weighted Round-Robin (WRR), strict priority, or a combination of strict and weighted queuing | GC   |
| <code>queue weight</code>                | Assigns round-robin weights to the priority queues  | GC   |
| <code>switchport priority default</code> | Sets a port priority for incoming untagged frames   | IC   |
| <code>show interfaces switchport</code>  | Displays the administrative and operational status of an interface  | PE   |
| <code>show queue mode</code>             | Shows the current queue mode  | PE   |
| <code>show queue weight</code>           | Shows weights assigned to the weighted queues   | PE   |

**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 \(569\)](#)

[show queue mode \(571\)](#)

**queue weight** This command assigns weights to the eight 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...weight7*

**no queue weight**

*weight0...weight7* - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1-255)

### Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 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 ([page 568](#)).
- ◆ 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 - 7.

```
Console(config)#queue weight 1 2 3 4 5 6 7 8  
Console(config)#
```

### Related Commands

[queue mode \(568\)](#)

[show queue weight \(571\)](#)

**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 eight 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 2 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
Queue ID  Weight
-----  -
0         1
1         2
2         4
3         6
4         8
5        10
6        12
7        14
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 111: Priority Commands (Layer 3 and 4)**

| Command                                 | Function  | Mode |
|---|---|------|
| <code>qos map cos-dscp</code>           | Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for internal priority processing           | GC   |
| <code>qos map dscp-cos</code>           | Maps internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface | IC   |
| <code>qos map dscp-mutation</code>      | Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing              | GC   |
| <code>qos map phb-queue</code>          | Maps internal per-hop behavior values to hardware queues  | GC   |
| <code>qos map trust-mode</code>         | Sets QoS mapping to DSCP or CoS   | IC   |
| <code>show qos map cos-dscp</code>      | Shows ingress CoS to internal DSCP map  | PE   |
| <code>show qos map dscp-cos</code>      | Shows internal DSCP to egress CoS map   | PE   |
| <code>show qos map dscp-mutation</code> | Shows ingress DSCP to internal DSCP map   | PE   |
| <code>show qos map phb-queue</code>     | Shows internal per-hop behavior to hardware queue map   | PE   |
| <code>show qos map trust-mode</code>    | Shows the QoS mapping mode  | PE   |

\* 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 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 112: Default Mapping of CoS/CFI to Internal PHB/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) |

## Command Mode

Global Configuration

## Command Usage

- ◆ The default mapping of CoS to PHB values shown in Table 112 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 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)#
```

**qos map dscp-cos** This command maps internal per-hop behavior and drop precedence value pairs to CoS/CFI values used in tagged egress packets on a Layer 2 interface. Use the **no** form to restore the default settings.

**Syntax**

**qos map dscp-cos** *cos-value cfi-value* **from** *phb0 drop-precedence0 ... phb7 drop-precedence7*

**no map ip dscp** *phb0 drop-precedence0 ... phb7 drop-precedence7*

*cos-value* - CoS value in ingress packets. (Range: 0-7)

*cfi-value* - 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)

*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)

**DEFAULT SETTING**

**Table 113: Mapping Internal PHB/Drop Precedence to CoS/CFI Values**

| Drop Precedence         | 0 (green) | 1 (red) | 3 (yellow) |
|-------------------------|-----------|---------|------------|
| <b>Per-hop Behavior</b> |           |         |            |
| 0                       | (0,0)     | (0,0)   | (0,0)      |
| 1                       | (1,0)     | (1,0)   | (1,0)      |
| 2                       | (2,0)     | (2,0)   | (2,0)      |
| 3                       | (3,0)     | (3,0)   | (3,0)      |
| 4                       | (4,0)     | (4,0)   | (4,0)      |
| 5                       | (5,0)     | (5,0)   | (5,0)      |
| 6                       | (6,0)     | (6,0)   | (6,0)      |
| 7                       | (7,0)     | (7,0)   | (7,0)      |

**Command Mode**

Interface Configuration (Port)

**Command Usage**

- ◆ Enter a CoS/CFI value pair, followed by the keyword "from" and then four internal per-hop behavior and drop precedence value pairs separated by spaces.
- ◆ If the packet is forwarded with an 8021.Q tag, the priority value in the egress packet is modified based on the table shown above, or on similar values as modified by this command.

### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-cos 1 0 from 1 2
Console(config-if)#
```

**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 114: Default Mapping of DSCP Values to Internal PHB/Drop Values**

|                | ingress-dscp1 | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   |
|----------------|---------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| ingress-dscp10 |               |     |     |     |     |     |     |     |     |     |     |
| 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 |
| 4              |               | 5,0 | 5,1 | 5,0 | 5,3 | 5,0 | 5,1 | 6,0 | 5,3 | 6,0 | 6,1 |
| 5              |               | 6,0 | 6,3 | 6,0 | 6,1 | 6,0 | 6,3 | 7,0 | 7,1 | 7,0 | 7,3 |
| 6              |               | 7,0 | 7,1 | 7,0 | 7,3 |     |     |     |     |     |     |

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 114](#), note that the DSCP value for these packets is now set to 25 ( $3 \times 2^3 + 1$ ) 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

**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 115: Mapping Internal Per-hop Behavior to Hardware Queues**

|                  |   |   |   |   |   |   |   |   |
|------------------|---|---|---|---|---|---|---|---|
| Per-hop Behavior | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Hardware Queues  | 2 | 0 | 1 | 3 | 4 | 5 | 6 | 7 |

### 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.

### Example

```
Console(config)##qos map phb-queue 0 from 1 2 3  
Console(config)#
```

**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 570](#)) 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 570](#)) 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 ge1/1
Console(config-if)#qos map trust-mode dscp
Console(config-if)#
```

**show qos map cos-dscp** This command shows ingress CoS/CFI to internal DSCP map.

### Syntax

**show qos map cos-dscp interface** *interface*

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### Command Mode

Privileged Exec

### Example

```
Console#show qos map cos-dscp interface ethernet 1/5
CoS Information of Eth 1/5
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-cos** This command shows the internal DSCP to egress CoS map, which converts internal PHB/Drop Precedence to CoS values.

### Syntax

**show qos map dscp-cos interface** *interface*

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### Command Mode

Privileged Exec

### Command Usage

This map is only used if the packet is forwarded with a 8021.Q tag.

### Example

```

Console#show qos map dscp-cos interface ethernet 1/5
Information of Eth 1/5
dscp-cos map:
phb:  drop precedence  0 (green)  1 (red)  3 (yellow)
-----
0  :                    (0,0)    (0,0)    (0,0)
1  :                    (1,0)    (1,0)    (1,0)
2  :                    (2,0)    (2,0)    (2,0)
3  :                    (3,0)    (3,0)    (3,0)
4  :                    (4,0)    (4,0)    (4,0)
5  :                    (5,0)    (5,0)    (5,0)
6  :                    (6,0)    (6,0)    (6,0)
7  :                    (7,0)    (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 interface** *interface*

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

### 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 interface ethernet 1/5
Information of Eth 1/5
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)
4 :   (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (6,0) (5,3) (6,0) (6,1)
5 :   (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)
6 :   (7,0) (7,1) (7,0) (7,3)
Console#
```

**show qos map phb-queue** This command shows internal per-hop behavior to hardware queue map.

### Syntax

```
show qos map phb-queue interface interface
                               interface
                               ethernet unit/port
                                   unit - Unit identifier. (Range: 1)
                                   port - Port number. (Range: 1-12)
```

### Command Mode

Privileged Exec

### Example

```
Console#show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
PHB Queue Map:
PHB:      0    1    2    3    4    5    6    7
-----
Queue:    2    0    1    3    4    5    6    7
Console#
```

**show qos map trust-mode** 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: 1-12)
```

## 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 116: Quality of Service Commands**

| Command                         | Function   | Mode |
|---------------------------------|--|------|
| <code>class-map</code>          | Creates a class map for a type of traffic  | GC   |
| <code>description</code>        | Specifies the description of a class map   | CM   |
| <code>match</code>              | Defines the criteria used to classify traffic  | CM   |
| <code>rename</code>             | Redefines the name of a class map  | CM   |
| <code>policy-map</code>         | Creates a policy map for multiple interfaces   | GC   |
| <code>bundle</code>             | Sets maximum ingress rate for a group of traffic flows   | PM   |
| <code>class</code>              | Defines a traffic classification for the policy to act on  | PM   |
| <code>description</code>        | Specifies the description of a policy map  | PM   |
| <code>rename</code>             | Redefines the name of a policy map   | PM   |
| <code>police flow</code>        | Defines an enforcer for classified traffic based on a metered flow rate                                    | PM-C |
| <code>police srtcm-color</code> | Defines an enforcer for classified traffic based on a single rate three color meter                        | PM-C |
| <code>police trtcm-color</code> | Defines an enforcer for classified traffic based on a two rate three color meter                           | PM-C |
| <code>priority</code>           | Sets the priority for the designated traffic flow  | PM-C |
| <code>set cos</code>            | Services IP traffic by setting a class of service value for matching packets for internal processing       | PM-C |
| <code>set ip dscp</code>        | Services IP traffic by setting a IP DSCP value for matching packets for internal processing                | PM-C |
| <code>set phb</code>            | Services IP traffic by setting a per-hop behavior value for matching packets for internal processing       | PM-C |
| <code>service-policy</code>     | Applies a policy map defined by the <code>policy-map</code> command to the input of a particular interface | IC   |
| <code>show class-map</code>     | Displays the QoS class maps which define matching criteria used for classifying traffic                    | PE   |

Table 116: Quality of Service Commands (Continued)

| Command                                | Function   | Mode |
|--|--|------|
| <code>show policy-map</code>           | Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations | PE   |
| <code>show policy-map interface</code> | Displays the configuration of all classes configured for all service policies on the specified interface                                   | PE   |

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, or a source port.
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 16 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

**[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**

match-any

**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 588](#)). The policy map is then bound by a service policy to an interface ([page 600](#)). 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 \(601\)](#)

**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

```
[no] match {access-list acl-name | cos cos | ip dscp dscp |
ip precedence ip-precedence | ipv6 dscp dscp | source-port interface|
vlan vlan}
```

*acl-name* - Name of the access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 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: 1-12)

*vlan* - 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.
- ◆ If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- ◆ If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- ◆ 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.

```
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 588](#)) 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 cos 0
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#

```

**bundle** This command sets the maximum flow rate for a group of traffic flows. Use the **no** form to remove a bundle.

### Syntax

**bundle** *index bundle-rate class-map1 class-map2 [class-map3... class-map5]*

*index* - Index for group of class maps. (Range: 1-3)

*bundle-rate* - Maximum flow rate for a group of traffic flows.  
(Range: 0-1,000,000 kbps)

*class-map* - Name of a class map. (Range: 1-32 characters)

### Default Setting

None

### Command Mode

Policy Map Configuration

### Command Usage

- ◆ This command will only be accepted if the meter mode specified for the class map members is set to one of the flow options ([police flow](#), [police srtpm-color](#), or [police trtpm-color](#)), and the violate action is set to drop any traffic exceeding the specified bundle rate.
- ◆ After binding a policy map for a traffic flow bundle to an interface, the switch will monitor the ingress rate for the bundle once every second.

### Example

```
Console(config)#policy-map rd-policy
Console(config-pmap)#bundle 1 100 rd-class finance-class marketing-class
Console(config-pmap)#
```

**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(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 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

```
[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 16 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 (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).

The token bucket C is initially full, that is, the token count  $Tc(0) = BC$ . Thereafter, the token count  $Tc$  is updated CIR times per second as follows:

- If  $Tc$  is less than BC,  $Tc$  is incremented by one, else

- Tc is not incremented.

When a packet of size B bytes arrives at time t, the following happens:

- If  $Tc(t) - B \geq 0$ , the packet is green and Tc is decremented by B down to the minimum value of 0, else
- else the packet is red and Tc 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
violate-action 0
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: 0-16000000 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 16 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  $T_c(0) = BC$  and the token count  $T_e(0) = BE$ . Thereafter, the token counts  $T_c$  and  $T_e$  are updated CIR times per second as follows:

- If  $T_c$  is less than BC,  $T_c$  is incremented by one, else
- if  $T_e$  is less than BE,  $T_e$  is incremented by one, else
- neither  $T_c$  nor  $T_e$  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  $Tc(t) - B \geq 0$ , the packet is green and Tc is decremented by B down to the minimum value of 0, else
- if  $Te(t) - B \geq 0$ , 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  $Tc(t) - B \geq 0$ , 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
- $Te(t) - B \geq 0$ , 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: 0-1000000 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 16 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  $T_p(0) = BP$  and the token count  $T_c(0) = BC$ . Thereafter, the token count  $T_p$  is incremented by one PIR times per second up to BP and the token count  $T_c$  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  $T_p(t) - B < 0$ , the packet is red, else
- 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.

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 a 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, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```

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 100000 6000
    conform-action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#

```

**priority** This command sets the priority for the designated traffic flow. Use the **no** form to restore the default setting.

**Syntax**

**priority** *priority*

**no priority**

*priority* - Priority assigned to designated traffic flow. (Range: 0-1000)

**Default Setting**

None

**Command Mode**

Policy Map Class Configuration

**Command Usage**

This command is used to set the priority of a policy-based class map.

**Example**

```

Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#priority 100
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.

```
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 10000 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

```
[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 10000 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 114, "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 trtcm-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 10000 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 or egress side of a particular interface. Use the `no` form to remove this mapping.

**Syntax**

**[no] service-policy {input | output} *policy-map-name***

**input** - Apply to the input traffic.

**output** - Apply to the output 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, Port Channel)

**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.

**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 ingress or egress 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** | **output**}

*interface*

*unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**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 117: Multicast Filtering Commands**

| Command Group                 | Function   |
|-------------------------------|--|
| IGMP Snooping                 | 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 |
| Static Multicast Routing      | Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs   |
| IGMP Filtering and Throttling | Configures IGMP filtering and throttling   |
| MLD Snooping                  | Configures Multicast Listener Discovery snooping for IPv6  |
| MLD Filtering and Throttling  | Configures MLD filtering and throttling for IPv6.  |
| MVR for IPv4                  | 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                                 |
| MVR for IPv6                  | 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                                 |

## IGMP Snooping

This section describes commands used to configure IGMP snooping on the switch.

**Table 118: IGMP Snooping Commands**

| Command  | Function   | Mode |
|--|--|------|
| <code>ip igmp snooping</code>                                | Enables IGMP snooping  | GC   |
| <code>ip igmp snooping priority</code>                       | Assigns a priority to all multicast traffic  | GC   |
| <code>ip igmp snooping proxy-reporting</code>                | Enables IGMP Snooping with Proxy Reporting   | GC   |
| <code>ip igmp snooping querier</code>                        | Allows this device to act as the querier for IGMP snooping   | GC   |
| <code>ip igmp snooping router-alert-option-check</code>      | Discards any IGMPv2/v3 packets that do not include the Router Alert option   | GC   |
| <code>ip igmp snooping router-port-expire-time</code>        | Configures the querier timeout   | GC   |
| <code>ip igmp report-limit</code>                            | Sets the IGMP report limit for an interface  | GC   |
| <code>ip igmp snooping tcn-flood</code>                      | Floods multicast traffic when a Spanning Tree topology change occurs   | GC   |
| <code>ip igmp snooping tcn-query-solicit</code>              | Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs   | GC   |
| <code>ip igmp snooping unregistered-data-flood</code>        | Floods unregistered multicast traffic into the attached VLAN   | GC   |
| <code>ip igmp snooping unsolicited-report-interval</code>    | Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)                                  | GC   |
| <code>ip igmp snooping version</code>                        | Configures the IGMP version for snooping   | GC   |
| <code>ip igmp snooping version-exclusive</code>              | Discards received IGMP messages which use a version different to that currently configured   | GC   |
| <code>ip igmp snooping vlan general-query-suppression</code> | Suppresses general queries except for ports attached to downstream multicast hosts   | GC   |
| <code>ip igmp snooping vlan immediate-leave</code>           | 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 | GC   |
| <code>ip igmp snooping vlan last-memb-query-count</code>     | Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members                              | GC   |
| <code>ip igmp snooping vlan last-memb-query-intvl</code>     | Configures the last-member-query interval  | GC   |
| <code>ip igmp snooping vlan mrd</code>                       | Sends multicast router solicitation messages   | GC   |
| <code>ip igmp snooping vlan proxy-address</code>             | Configures a static address for proxy IGMP query and reporting   | GC   |
| <code>ip igmp snooping vlan proxy-reporting</code>           | Enables IGMP Snooping with Proxy Reporting   | GC   |
| <code>ip igmp snooping vlan query-interval</code>            | Configures the interval between sending IGMP general queries   | GC   |

Table 118: IGMP Snooping Commands (Continued)

| Command  | Function   | Mode |
|--|--|------|
| <code>ip igmp snooping vlan query-resp-intvl</code>  | Configures the maximum time the system waits for a response to general queries             | GC   |
| <code>ip igmp snooping vlan static</code>            | Adds an interface as a member of a multicast group   | GC   |
| <code>ip igmp snooping vlan version</code>           | Configures the IGMP version for snooping   | GC   |
| <code>ip igmp snooping vlan version-exclusive</code> | Discards received IGMP messages which use a version different to that currently configured | GC   |
| <code>clear ip igmp snooping groups dynamic</code>   | Clears multicast group information dynamically learned through IGMP snooping               | PE   |
| <code>clear ip igmp snooping statistics</code>       | Clears IGMP snooping statistics  | PE   |
| <code>show ip igmp snooping</code>                   | Shows the IGMP snooping, proxy, and query configuration                                    | PE   |
| <code>show ip igmp snooping group</code>             | Shows known multicast group, source, and host port mapping                                 | PE   |
| <code>show ip igmp snooping mrouter</code>           | Shows multicast router ports   | PE   |
| <code>show ip igmp snooping statistics</code>        | Shows IGMP snooping protocol statistics for the specified interface                        | PE   |

**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 \(622\)](#)

**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

- ◆ IGMP snooping querier is not supported for IGMPv3 snooping (see [ip igmp snooping version](#)).
- ◆ 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(config)#ip igmp snooping router-alert-option-check  
Console(config)#
```

**ip igmp snooping router-port-expire-time** This command configures the querier timeout. 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 timeout to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

**ip igmp report-limit** This command sets the maximum rate at which IGMP membership reports can be sent from an interface. Use the **no** form to restore the default setting.

**ip igmp report-limit rate** *rate interface*

**no ip igmp report-limit** [*interface*]

*rate* - The rate at which IGMP membership reports can be sent from an interface. (Range: 5-255 pps)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

#### Default Setting

255 pps

#### Command Mode

Global Configuration

### Command Usage

Membership reports exceeding the configured limits for the interface are dropped. This command can be used to prevent DoS attacks.

### Example

```
Console(config)#ip igmp rate-limit rate 100 interface ethernet 1/1  
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 timeout 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 607](#)).

### Example

```
Console(config)#ip igmp snooping unsolicited-report-interval 5  
Console(config)#
```

**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 timeout period. (The time out for this release is defined by Last Member Query Interval (fixed at one second) \* Robustness Variable (fixed at 2) as defined in RFC 2236.
- ◆ If immediate-leave is used, 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 607](#)).

**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 607).

### 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 607](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 607](#)).

### 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 607](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 607](#)).

### 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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 through IGMP snooping. Statically configured multicast address are not cleared.

### Example

```
Console#clear ip igmp snooping groups dynamic
Console#
```

**clear ip igmp snooping statistics** This command clears IGMP snooping statistics.

### Syntax

**clear ip igmp snooping statistics** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**vlan** *vlan-id* - VLAN identifier (Range: 1-4094)

### Command Mode

Privileged Exec

### Example

```
Console#clear ip igmp snooping statistics
Console#
```

**show ip igmp snooping** This command shows the IGMP snooping, proxy, and query configuration settings.

### Syntax

**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#show ip igmp snooping
IGMP Snooping                : Enabled
Router Port Expire Time      : 300 s
Router Alert Check           : Disabled
Router Port Mode              : Forward
TCN Flood                     : Disabled
TCN Query Solicit            : Disabled
Unregistered Data Flood      : Disabled
802.1p Forwarding Priority    : Disabled
Unsolicited Report Interval  : 400 s
Version Exclusive            : Disabled
Version                       : 2
Proxy Reporting               : Disabled
Querier                       : Disabled

VLAN 1:
-----
IGMP Snooping                : Enabled
IGMP Snooping Running Status : Inactive
Version                       : Using global Version (2)
Version Exclusive             : Using global status (Disabled)
Immediate Leave                : Disabled
Last Member Query Interval    : 10 (unit: 1/10s)
Last Member Query Count       : 2
General Query Suppression     : Disabled
Query Interval                 : 125
Query Response Interval       : 100 (unit: 1/10s)
Proxy Query Address            : 0.0.0.0
Proxy Reporting                : Using global status (Disabled)
Multicast Router Discovery     : Disabled

VLAN Static Group   Port
-----
1      224.1.1.1     Eth 1/ 1
:

```

**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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**igmpsnp** - Display only entries learned through IGMP snooping.

**sort-by-port** - Display entries sorted by port.

**user** - Display only the user-configured multicast entries.

*vlan-id* - VLAN ID (1-4094)

### 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).

VLAN Group          Port          Up time      Expire Count
-----
  1 224.1.1.1
      Eth 1/ 1 (R)      00:00:00:37      2 (P)
      Eth 1/ 2 (M)
      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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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#

```

**Table 119: show ip igmp snooping statistics input - display description**

| Field         | Description   |
|---------------|---|
| Interface     | Shows interface.  |
| Report        | The number of IGMP membership reports received on this interface.   |
| Leave         | The number of leave messages received on this interface.  |
| G Query       | The number of general query messages received on this interface.  |
| G(-S)-S Query | The number of group specific or group-and-source specific query messages received on this interface.  |
| Drop          | 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. |
| Join Succ     | The number of times a multicast group was successfully joined.  |
| Group         | The number of multicast groups active on this interface.  |

The following shows IGMP protocol statistics output:

```

Console#show ip igmp snooping statistics output interface ethernet 1/1
Output Statistics:
Interface  Report  Leave  G Query  G(-S)-S Query  Drop  Group
-----
Eth 1/ 1   12      0      1         0         0      0

Console#

```

**Table 120: show ip igmp snooping statistics output - display description**

| Field         | Description   |
|---------------|---|
| Interface     | Shows interface.  |
| Report        | The number of IGMP membership reports sent from this interface.   |
| Leave         | The number of leave messages sent from this interface.  |
| G Query       | The number of general query messages sent from this interface.  |
| G(-S)-S Query | The number of group specific or group-and-source specific query messages sent from this interface.  |
| Drop          | 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. |
| Group         | The number of multicast groups active on this interface.  |

The following shows IGMP query-related statistics for VLAN 1:

```

Console#show ip igmp snooping statistics query vlan 1
Other Querier           : None
Other Querier Expire    : 0(m):0(s)
Other Querier Uptime    : 0(h):0(m):0(s)
Self Querier            : 192.168.2.13
Self Querier Expire     : 0(m):0(s)
Self Querier Uptime     : 0(h):0(m):0(s)
General Query Received  : 0
General Query Sent      : 0
Specific Query Received : 0
Specific Query Sent     : 0
Warn Rate Limit         : 0 sec.
V1 Warning Count        : 0
V2 Warning Count        : 0
V3 Warning Count        : 0
Console#

```

**Table 121: show ip igmp snooping statistics vlan query - display description**

| Field                   | Description  |
|-------------------------|--|
| Other Querier           | IP address of remote querier on this interface.  |
| Other Querier Expire    | Time after which remote querier is assumed to have expired.  |
| Other Querier Uptime    | Time remote querier has been up.   |
| Self Querier            | IP address of local querier on this interface.   |
| Self Querier Expire     | Time after which local querier is assumed to have expired.   |
| Self Querier Uptime     | Time local querier has been up.  |
| General Query Received  | The number of general queries received on this interface.  |
| General Query Sent      | The number of general queries sent from this interface.  |
| Specific Query Received | The number of specific queries received on this interface.   |
| Specific Query Sent     | The number of specific queries sent from this interface.   |
| Warn Rate Limit         | 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. |
| V1 Warning Count        | The number of times the query version received (Version 1) does not match the version configured for this interface.   |
| V2 Warning Count        | The number of times the query version received (Version 2) does not match the version configured for this interface.   |
| V3 Warning Count        | The number of times the query version received (Version 3) does not match the version configured for this interface.   |

## Static Multicast Routing

This section describes commands used to configure static multicast routing on the switch.

**Table 122: Static Multicast Interface Commands**

| Command                                    | Function                     | Mode |
|--|------------------------------|------|
| <code>ip igmp snooping vlan mrouter</code> | Adds a multicast router port | GC   |
| <code>show ip igmp snooping mrouter</code> | Shows multicast router ports | PE   |

**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*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 10 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
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 123: IGMP Filtering and Throttling Commands**

| Command                                      | Function   | Mode |
|--|--|------|
| <code>ip igmp filter</code>                  | Enables IGMP filtering and throttling on the switch                        | GC   |
| <code>ip igmp profile</code>                 | Sets a profile number and enters IGMP filter profile configuration mode    | GC   |
| <code>ip igmp rate-limit</code>              | Sets the maximum rate at which IGMP reports can be sent from an interface  | GC   |
| <code>permit, deny</code>                    | Sets a profile access mode to permit or deny                               | IPC  |
| <code>range</code>                           | Specifies one or a range of multicast addresses for a profile              | IPC  |
| <code>ip igmp authentication</code>          | Enables RADIUS authentication for IGMP JOIN requests.                      | IC   |
| <code>ip igmp filter</code>                  | Assigns an IGMP filter profile to an interface                             | IC   |
| <code>ip igmp max-groups</code>              | Specifies an IGMP throttling number for an interface                       | IC   |
| <code>ip igmp max-groups action</code>       | Sets the IGMP throttling action for an interface                           | IC   |
| <code>ip multicast-data-drop</code>          | Drops all multicast data packets   | IC   |
| <code>show ip igmp authentication</code>     | Displays the IGMP authentication setting for interfaces                    | PE   |
| <code>show ip igmp filter</code>             | Displays the IGMP filtering status   | PE   |
| <code>show ip igmp profile</code>            | Displays IGMP profiles and settings  | PE   |
| <code>show ip igmp rate-limit</code>         | Shows the maximum rate at which IGMP reports can be sent from an interface | PE   |
| <code>show ip igmp throttle interface</code> | Displays the IGMP throttling setting for interfaces                        | PE   |
| <code>show ip multicast-data-drop</code>     | Shows if the interface is configured to drop multicast data packets        | PE   |

**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

**[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

**[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)#
```

**ip igmp rate-limit** This command sets the maximum rate at which IGMP membership reports can be sent from an interface. Use the **no** form to restore the default setting.

**ip igmp rate-limit rate** *rate interface*

**no ip igmp rate-limit** [*interface*]

*rate* - The rate at which IGMP membership reports can be sent from an interface. (Range: 5-255 pps)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### Default Setting

255

### Command Mode

Global Configuration

### Command Usage

Membership reports exceeding the configured limits for the interface are dropped. This command can be used to prevent DoS attacks.

### Example

```
Console(config)#ip igmp rate-limit rate 100 interface ethernet 1/1
Console(config)#
```

**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
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 124: IGMP Authentication RADIUS Attribute Value Pairs**

| Attribute Name    | AVP Type | Entry              |
|-------------------|----------|--------------------|
| USER_NAME         | 1        | User MAC address   |
| USER_PASSWORD     | 2        | User MAC address   |
| NAS_IP_ADDRESS    | 4        | Switch IP address  |
| NAS_PORT          | 5        | User Port Number   |
| FRAMED_IP_ADDRESS | 8        | Multicast Group ID |

### Example

This example shows how to enable IGMP Authentication on all of the switch's Ethernet interfaces.

```
Console(config)#interface ethernet 1/1-12
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: 1-1024)

## Default Setting

1024

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## 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” (see the [ip igmp max-groups action](#) command). 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(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

**ip igmp max-groups action** 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(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

**ip multicast-data-drop** This command drops all multicast data packets. Use the **no** form to disable this feature.

### Syntax

**[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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

#### 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 1/11: Enabled
Ethernet 1/12: Enabled
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: 1-12)  
port-channel channel-id (Range: 1-12)
```

### 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 rate-limit** This command shows the maximum rate at which IGMP membership reports can be sent from an interface.

### Syntax

**show ip igmp rate-limit** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 rate-limit interface vlan 1
Interface Rate Limit (pps)
-----
VLAN      1                255
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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

#### 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 : 1024
                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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

#### 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 125: MLD Snooping Commands**

| Command  | Function   | Mode |
|--|--|------|
| <code>ipv6 mld snooping</code>                         | Enables MLD Snooping globally                                      | GC   |
| <code>ipv6 mld snooping proxy-reporting</code>         | Enables MLD Snooping with Proxy Reporting                          | GC   |
| <code>ipv6 mld snooping querier</code>                 | Allows the switch to act as the querier for MLD snooping           | GC   |
| <code>ipv6 mld snooping query-interval</code>          | Configures the interval between sending MLD general query messages | GC   |
| <code>ipv6 mld snooping query-max-response-time</code> | Configures the maximum response time for a general queries         | GC   |
| <code>ipv6 mld snooping robustness</code>              | Configures the robustness variable                                 | GC   |
| <code>ipv6 mld snooping router-port-expire-time</code> | Configures the router port expire time                             | GC   |
| <code>ipv6 mld snooping unknown-multicast mode</code>  | Sets an action for unknown multicast packets                       | GC   |

**Table 125: MLD Snooping Commands** (Continued)

| Command  | Function   | Mode |
|--|--|------|
| <code>ipv6 mld snooping unsolicited-report-interval</code> | Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)                                | GC   |
| <code>ipv6 mld snooping version</code>                     | Configures the MLD Snooping version  | GC   |
| <code>ipv6 mld snooping vlan immediate-leave</code>        | Removes a member port of an IPv6 multicast service if a leave packet is received at that port and MLD immediate-leave is enabled for the parent VLAN | GC   |
| <code>ipv6 mld snooping vlan mrouter</code>                | Adds an IPv6 multicast router port   | GC   |
| <code>ipv6 mld snooping vlan static</code>                 | Adds an interface as a member of a multicast group   | GC   |
| <code>clear ip igmp snooping groups dynamic</code>         | Clears multicast group information dynamically learned through MLD snooping or MVR6  | PE   |
| <code>clear ip igmp snooping statistics</code>             | Clears clears IGMP snooping statistics   | PE   |
| <code>show ipv6 mld snooping</code>                        | Displays MLD Snooping configuration  | PE   |
| <code>show ipv6 mld snooping group</code>                  | Displays the learned groups  | PE   |
| <code>show ipv6 mld snooping group source-list</code>      | Displays the learned groups and corresponding source list  | PE   |
| <code>show ipv6 mld snooping mrouter</code>                | Displays the information of multicast router ports   | PE   |
| <code>show ipv6 mld snooping statistics</code>             | Shows IGMP snooping protocol statistics for the specified interface  | PE   |

**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
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.

#### Example

```
Console(config)#ipv6 mld snooping proxy-reporting
Console(config)#
```

**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

#### 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 150  
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 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

#### 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.

### 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 643](#)).

### 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)#
```

**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* - Stack unit. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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  
**vlan static** 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::X)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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** This command clears multicast group information dynamically learned through  
**snooping groups** MLD snooping.  
**dynamic**

### Syntax

**clear ipv6 mld snooping groups dynamic**

### Command Mode

Privileged Exec

### Command Usage

This command only clears entries learned through 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: 1-12)
        port-channel channel-id (Range: 1-12)
        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
Unsolicited Report Interval : 400 sec
Immediate Leave           : Disabled on all VLAN
```

```
MLD Snooping Version          : Version 2  
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:

```
Console#show ipv6 mld snooping group  
  
Total Entries 3, limit 255  
  
VLAN Multicast IPv6 Address          Member port Type  
-----  
1 FF02::01:01:01:01                 Eth 1/1      MLD Snooping  
1 FF02::01:01:01:02                 Eth 1/1      Multicast Data  
1 FF02::01:01:01:02                 Eth 1/1      User  
  
Console#
```

**show ipv6 mld snooping group source-list** 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** [*ipv6-address* | **vlan** *vlan-id*]

*ipv6-address* - An IPv6 address of a multicast group. (Format: X:X:X:X::X)

*vlan-id* - VLAN identifier (1-4094)

### Command Mode

Privileged Exec

### Example

The following shows MLD Snooping group mapping information:

```
Console#show ipv6 mld snooping group source-list  
  
VLAN ID          : 1  
Multicast IPv6 Address : FF02::01:01:01:01  
Member Port      : Eth 1/1  
Type             : MLD Snooping
```

```

Filter Mode                : Include
(if exclude filter mode)
Filter Timer elapse       : 10 sec.
Request List              : ::01:02:03:04, ::01:02:03:05, ::01:02:03:06,
                          ::01:02:03:07
Exclude List              : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                          ::02:02:03:07
(if include filter mode)
Include List              : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                          ::02:02:03:06

```

```

Option:
  Filter Mode: Include, Exclude

```

```

Console#

```

**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**

**{input [interface *interface*] |**

**output [interface *interface*] |**

**query [vlan *vlan-id*] |**

**summary interface *interface*}**

*interface*

**ethernet *unit/port***

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel *channel-id*** (Range: 1-12)

**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 126: MLD Filtering and Throttling Commands**

| Command                                       | Function   | Mode |
|---|--|------|
| <code>ipv6 mld filter</code>                  | Enables MLD filtering and throttling on the switch                     | GC   |
| <code>ipv6 mld profile</code>                 | Sets a profile number and enters MLD filter profile configuration mode | GC   |
| <code>permit, deny</code>                     | Sets a profile access mode to permit or deny                           | IPC  |
| <code>range</code>                            | Specifies one or a range of multicast addresses for a profile          | IPC  |
| <code>ipv6 mld filter</code>                  | Assigns an MLD filter profile to an interface                          | IC   |
| <code>ipv6 mld max-groups</code>              | Specifies an M:D throttling number for an interface                    | IC   |
| <code>ipv6 mld max-groups action</code>       | Sets the MLD throttling action for an interface                        | IC   |
| <code>ipv6 mld query-drop</code>              | Drops any received MLD query packets                                   | IC   |
| <code>ipv6 multicast-data-drop</code>         | Enable multicast data guard mode on a port interface                   | IC   |
| <code>show ipv6 mld filter</code>             | Displays the MLD filtering status                                      | PE   |
| <code>show ipv6 mld profile</code>            | Displays MLD profiles and settings                                     | PE   |
| <code>show ipv6 mld query-drop</code>         | Shows if the interface is configured to drop MLD query packets         | PE   |
| <code>show ipv6 mld throttle interface</code> | Displays the MLD throttling setting for interfaces                     | PE   |

**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 MVR 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

```
[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
Console(config-mld-profile)#
```

**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

**[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.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld filter 19
Console(config-if)#
```

**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: 1-1024)

### Default Setting

1024

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### 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 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)

### 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.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld query-drop
Console(config-if)#
```

**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

```
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: 1-12)  
port-channel channel-id (Range: 1-12)
```

### Default Setting

None

### Command Mode

Privileged Exec

### Example

```
Console#show ipv6 mld filter  
MLD filter Enabled  
Console#show ipv6 mld filter interface ethernet 1/3  
Ethernet 1/3 information  
-----  
MLD Profile 19  
Deny  
Range ff05::101 ff05::103  
Console#
```

**show ipv6 mld profile** This command displays MLD filtering profiles created on the switch.

### Syntax

```
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
```

```
Console#show ipv6 mld profile 5
MLD Profile 19
Deny
Range ff05::101          ff05::103
```

**show ipv6 mld query-drop** This command shows if the specified interface is configured to drop MLD query packets.

#### Syntax

**show ipv6 mld query-drop interface** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

#### 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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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#
```

## MVR 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 127: Multicast VLAN Registration for IPv4 Commands**

| Command                                   | Function   | Mode |
|---|--|------|
| <code>mvr</code>                          | Globally enables MVR   | GC   |
| <code>mvr associated-profile</code>       | Binds the MVR group addresses specified in a profile to an MVR domain  | GC   |
| <code>mvr domain</code>                   | Enables MVR for a specific domain  | GC   |
| <code>mvr priority</code>                 | Assigns a priority to all multicast traffic in the MVR VLAN  | GC   |
| <code>mvr profile</code>                  | Maps a range of MVR group addresses to a profile   | GC   |
| <code>mvr proxy-query-interval</code>     | Configures the interval at which the receiver port sends out general queries.  | GC   |
| <code>mvr proxy-switching</code>          | 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                                  | GC   |
| <code>mvr robustness-value</code>         | Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries   | GC   |
| <code>mvr source-port-mode dynamic</code> | Configures the switch to only forward multicast streams which the source port has dynamically joined   | GC   |
| <code>mvr upstream-source-ip</code>       | Configures the source IP address assigned to all control packets sent upstream   | GC   |
| <code>mvr vlan</code>                     | Specifies the VLAN through which MVR multicast data is received  | GC   |
| <code>mvr immediate-leave</code>          | Enables immediate leave capability   | IC   |
| <code>mvr type</code>                     | Configures an interface as an MVR receiver or source port  | IC   |
| <code>mvr vlan group</code>               | Statically binds a multicast group to a port   | IC   |
| <code>clear mrv groups dynamic</code>     | Clears multicast group information dynamically learned through MVR   | PE   |
| <code>clear mrv statistics</code>         | Clears MRV statistics  | PE   |
| <code>show mvr</code>                     | 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 | PE   |
| <code>show mvr associated-profile</code>  | Shows the profiles bound the specified domain  | PE   |

**Table 127: Multicast VLAN Registration for IPv4 Commands** (Continued)

| Command                          | Function   | Mode |
|----------------------------------|--|------|
| <code>show mvr interface</code>  | Shows MVR settings for interfaces attached to the MVR VLAN   | PE   |
| <code>show mvr members</code>    | Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address | PE   |
| <code>show mvr profile</code>    | Shows all configured MVR profiles  | PE   |
| <code>show mvr statistics</code> | Shows MVR protocol statistics for the specified interface  | PE   |

**mvr** This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the **no** form of this command to globally disable MVR.

### Syntax

**[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.

```
Console(config)#mvr
Console(config)#
```

**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

**[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 \(667\)](#)

**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 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)

### 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 1024 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

**[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 \(670\)](#)

**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 \(669\)](#)

**mvr 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] 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**

*domain-id* - An independent multicast domain. (Range: 1-5)

### 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.
- ◆ 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
Console(config-if)#
```

**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

**[no] 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 mrv groups dynamic** This command clears multicast group information dynamically learned through MVR.

#### Syntax

**clear mrv groups dynamic**

#### Command Mode

Privileged Exec

#### Command Usage

This command only clears entries learned through MRV. Statically configured multicast addresses are not cleared.

#### Example

```
Console#clear mrv groups dynamic
Console#
```

**clear mrv statistics** This command clears MVR statistics.

#### Syntax

**clear mrv statistics** [**interface** *interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**vlan** *vlan-id* - VLAN identifier (Range: 1-4094)

#### Command Mode

Privileged Exec

#### Example

```
Console#clear ip igmp snooping 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 128: show mvr - display description**

| Field                          | Description   |
|--------------------------------|---|
| MVR 802.1p Forwarding Priority | Priority assigned to multicast traffic forwarded into the MVR VLAN  |
| MVR Proxy Switching            | Shows if MVR proxy switching is enabled   |
| MVR Robustness Value           | Shows the number of reports or query messages sent when proxy switching is enabled  |
| MVR Proxy Query Interval       | Shows the interval at which the receiver port sends out general queries   |
| MVR Source Port Mode           | Shows if the switch forwards all multicast streams, or only those which the source port has dynamically joined  |
| MVR Domain                     | An independent multicast domain.  |
| MVR Config Status              | Shows if MVR is globally enabled on the switch.   |
| MVR Running Status             | Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.) |

Table 128: show mvr - display description (Continued)

| Field                      | Description   |
|----------------------------|---|
| MVR Multicast VLAN         | Shows the VLAN used to transport all MVR multicast traffic.     |
| MVR Current Learned Groups | The current number of MVR group addresses                       |
| MVR Upstream Source IP     | The source IP address assigned to all upstream control packets. |

**show mvr associated-profile** This command shows the profiles bound the specified domain.

#### Syntax

**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

**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

### 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)
Eth1/ 3 Source  Inactive/Discarding
Eth1/ 1 Receiver Active/Forwarding    Disabled      225.0.0.1 (VLAN1)
                                                    225.0.0.9 (VLAN3)

Eth1/ 4      Receiver  Active/Down        Disabled
Console#

```

**Table 129: show mvr interface - display description**

| Field                | Description  |
|----------------------|--|
| MVR Domain           | An independent multicast domain.   |
| Port                 | Shows interfaces attached to the MVR.  |
| Type                 | Shows the MVR port type.   |
| Status               | 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. |
| Immediate            | Shows if immediate leave is enabled or disabled.   |
| Static Group Address | Shows any static MVR group assigned to an interface, and the receiver VLAN.  |

**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] | sort-by-port [interface]]
```

*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.

**sort-by-port** - The multicast groups associated with an interface.

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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).
Uptime: Group elapsed time; Expire: Group remain time.
Expire : Group remaining time (m:s).

Group Address   VLAN Port           Uptime           Expire Count
-----
234.5.6.7      1
                1 Eth 1/ 2(S)
                2 Eth 1/ 2(R)
                00:20           1(P)

Console#

```

**Table 130: show mvr members - display description**

| Field         | Description   |
|---------------|---|
| Group Address | Multicast group address.  |
| VLAN          | VLAN to which this address is forwarded.                            |
| Port          | Port to which this address is forwarded.                            |
| Uptime        | Time that this multicast group has been known.                      |
| Expire        | The time until this entry expires.                                  |
| Count         | The number of times this address has been learned by IGMP snooping. |

**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  
input [interface interface] | output [interface interface] |  
query | summary interface [interface] | mvr-vlan
```

*domain-id* - An independent multicast domain. (Range: 1-5)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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 131: show mvr statistics input - display description**

| Field     | Description   |
|-----------|---|
| Interface | Shows interfaces attached to the MVR.                             |
| Report    | The number of IGMP membership reports received on this interface. |
| Leave     | The number of leave messages received on this interface.          |
| G Query   | The number of general query messages received on this interface.  |

**Table 131: show mvr statistics input - display description** (Continued)

| Field         | Description   |
|---------------|---|
| G(-S)-S Query | The number of group specific or group-and-source specific query messages received on this interface.  |
| Drop          | 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 |
| Join Succ     | The number of times a multicast group was successfully joined.  |
| Group         | The number of MVR groups active on this interface.  |

The following shows MVR protocol-related statistics sent:

```

Console#show mvr domain 1 statistics output
MVR Domain : 1 , MVR VLAN: 1
Output Statistics:
Interface  Report  Leave   G Query  G(-S)-S Query Drop    Group
-----
Eth 1/ 1   12      0       1        0        0      0
Eth 1/ 2   5       1       4        1        0      0
MVLAN  1    0       0       0        0        0      0
DVLAN  2    0       0       0        0        0      0
Console#

```

**Table 132: show mvr statistics output - display description**

| Field         | Description   |
|---------------|---|
| Interface     | Shows interfaces attached to the MVR.   |
| Report        | The number of IGMP membership reports sent from this interface.   |
| Leave         | The number of leave messages sent from this interface.  |
| G Query       | The number of general query messages sent from this interface.  |
| G(-S)-S Query | The number of group specific or group-and-source specific query messages sent from this interface.  |
| Drop          | 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 |
| Group         | The number of MVR groups active on this interface.  |

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):9(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
Console#

```

**Table 133: show mvr statistics query - display description**

| Field                   | Description   |
|-------------------------|---|
| Other Querier           | The IP address of the querier on this interface.  |
| Other Querier Expire    | The time after which this querier is assumed to have expired.                             |
| Other Querier Uptime    | Other querier's time up.  |
| Self Querier            | This querier's IP address.  |
| Self Querier Expire     | This querier's expire time.   |
| Self Querier Uptime     | This querier's time up.   |
| General Query Received  | The number of general queries received on this interface.                                 |
| General Query Sent      | The number of general queries sent from this interface.                                   |
| Specific Query Received | The number of specific queries received on this interface.                                |
| Specific Query Sent     | The number of specific queries sent from this interface.                                  |
| Warn Rate Limit         | Count down from 15 seconds after receiving a Query different from the configured version. |
| V# Warning Count        | Number of queries received on MVR that were configured for IGMP version 1, 2 or 3.        |

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       :
    General      : 0          Report       : 7
    Group Specific : 0          Leave        : 4
Received        :          Recieved       :
  General       : 0          Report       : 0
  Group Specific : 0          Leave        : 0
  V1 Warning Count: 0        Join Success  : 0
  V2 Warning Count: 0        Filter Drop   : 0
  V3 Warning Count: 0
                                   Source Port Drop: 0
                                   Others Drop    : 0

Console#

```

**Table 134: show mvr statistics summary interface - display description**

| Field            | Description  |
|------------------|--|
| Domain           | An independent multicast domain.   |
| Number of Groups | Number of groups learned on this port.   |
| Querier          |  |
| Transmit         |  |
| General          | Number of general queries transmitted.   |
| Group Specific   | Number of group specific queries transmitted.                                      |
| Received         |  |
| General          | Number of general queries received.  |
| Group Specific   | Number of group specific queries received.   |
| V# Warning Count | Number of queries received on MVR that were configured for IGMP version 1, 2 or 3. |
| Report & Leave   |  |
| Transmit         |  |
| Report           | Number of transmitted reports.   |
| Leave            | Number of transmitted leaves.  |
| Received         |  |
| Report           | Number of reports received.  |
| Leave            | Number of leaves received.   |
| Join Success     | Number of join reports processed successfully.                                     |
| Filter Drop      | Number of report/leave messages dropped by IGMP filter.                            |
| Source Port Drop | Number of report/leave messages dropped by MVR source port.                        |
| Others Drop      | Number of report/leave messages dropped for other reasons.                         |

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 135: show mvr statistics summary interface mvr vlan - description**

| Field            | Description   |
|------------------|---|
| Domain           | An independent multicast domain.  |
| Number of Groups | Number of groups learned on this port.  |
| Querier          |   |
| Other Querier    | Other IGMP querier's IP address.  |
| Other Expire     | Other querier's expire time.  |
| Other Uptime     | Other querier's time up.  |
| Self Querier     | This querier's IP address.  |
| Self Expire      | This querier's expire time.   |
| Self Uptime      | This querier's time up.   |
| Transmit         |   |
| General          | Number of general queries sent from receiver port.                                |
| Group Specific   | Number of group specific queries sent from receiver port.                         |
| Received         |   |
| General          | Number of general queries received.   |
| Group Specific   | Number of group specific queries received.  |
| V# Warning Count | Number of queries received on MVR that were configured by IGMP version 1, 2 or 3. |
| Report & Leave   |   |
| Host IP Addr     | Source IP address used to send report/leave messages from source port.            |

**Table 135: show mvr statistics summary interface mvr vlan - description**

| Field            | Description   |
|------------------|---|
| Unsolicit Expire | Expiration time for unsolicit reports sent out from source port |
| Transmit         |   |
| Report           | Number of reports sent out from source port.                    |
| Leave            | Number of leaves sent out from source port.                     |
| Received         | Field header  |
| Report           | Number of reports received.                                     |
| Leave            | Number of leaves received.                                      |
| Join Success     | Number of join reports processed successfully.                  |
| Filter Drop      | Number of report/leave messages dropped by IGMP filter.         |
| Source Port Drop | Number of report/leave messages dropped by MVR source port.     |
| Others Drop      | Number of report/leave messages dropped for other reasons.      |

## MVR 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 to 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 136: Multicast VLAN Registration for IPv6 Commands**

| Command                                | Function   | Mode |
|--|--|------|
| <code>mvr6 associated-profile</code>   | Binds the MVR6 group addresses specified in a profile to an MVR6 domain  | GC   |
| <code>mvr6 domain</code>               | Enables MVR6 for a specific domain   | GC   |
| <code>mvr6 priority</code>             | Assigns a priority to all multicast traffic in the MVR6 VLAN   | GC   |
| <code>mvr6 profile</code>              | Maps a range of MVR6 group addresses to a profile  | GC   |
| <code>mvr6 proxy-query-interval</code> | Configures the interval at which the receiver port sends out general queries.  | GC   |
| <code>mvr6 proxy-switching</code>      | Enables MVR6 proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled | GC   |
| <code>mvr6 robustness-value</code>     | Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries                           | GC   |

**Table 136: Multicast VLAN Registration for IPv6 Commands** (Continued)

| Command                                    | Function  | Mode |
|--|---|------|
| <code>mvr6 source-port-mode dynamic</code> | Configures the switch to only forward multicast streams which the source port has dynamically joined  | GC   |
| <code>mvr6 upstream-source-ip</code>       | Configures the source IP address assigned to all control packets sent upstream  | GC   |
| <code>mvr6 vlan</code>                     | Specifies the VLAN through which MVR6 multicast data is received  | GC   |
| <code>mvr6 immediate-leave</code>          | Enables immediate leave capability  | IC   |
| <code>mvr6 type</code>                     | Configures an interface as an MVR6 receiver or source port  | IC   |
| <code>mvr6 vlan group</code>               | Statically binds a multicast group to a port  | IC   |
| <code>clear mvr6 groups dynamic</code>     | Clears multicast group information dynamically learned through MVR6   | PE   |
| <code>clear mvr6 statistics</code>         | Clears the MVR6 statistics globally or on a per-interface basis.  | PE   |
| <code>show mvr6</code>                     | Shows information about MVR domain settings, including MVR6 operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address | PE   |
| <code>show mvr6 associated-profile</code>  | Shows the profiles bound the specified domain   | PE   |
| <code>show mvr6 interface</code>           | Shows MVR settings for interfaces attached to the MVR6 VLAN   | PE   |
| <code>show mvr6 members</code>             | Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address                                  | PE   |
| <code>show mvr6 profile</code>             | Shows all configured MVR6 profiles  | PE   |
| <code>show mvr6 statistics</code>          | Shows MVR6 protocol statistics for the specified interface  | PE   |

**mvr6 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

**[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:

```
Console(config)#mvr6 domain 1 associated-profile rd
Console(config)#
```

**mvr6 domain** This command enables Multicast VLAN Registration (MVR6) for a specific domain. Use the **no** form of this command to disable MVR6 for a domain.

### Syntax

**[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](#)

**mvr6 profile** 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 MVR VLAN. Any multicast data associated with an MVR 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 MVR share a maximum number of 1024 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 ff01:0:0:0:0:0:fe ff01:0:0:0:0:0: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 MVR 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 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 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 \(693\)](#)

**mvr6 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

**mvr6 robustness-value** *value*

**no mvr6 robustness-value**

*value* - The robustness used for all interfaces. (Range: 1-10)

### Default Setting

2

### 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 \(692\)](#)

**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(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

**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(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

**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**

*domain-id* - An independent multicast domain. (Range: 1-5)

### 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.
- ◆ 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 641](#)).
- ◆ 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 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 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.

```
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

**[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(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 through 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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**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 MVR6 statistics for 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 137: show mvr6 - display description**

| Field                           | Description   |
|---------------------------------|---|
| MVR6 802.1p Forwarding Priority | Priority assigned to multicast traffic forwarded into the MVR6 VLAN |
| MVR6 Proxy Switching            | Shows if MVR6 proxy switching is enabled                            |

**Table 137: show mvr6 - display description** (Continued)

| Field                     | Description   |
|---------------------------|---|
| MVR6 Robustness Value     | Shows the number of reports or query messages sent when proxy switching is enabled  |
| MVR6 Proxy Query Interval | The interval at which the receiver port sends out general queries   |
| MVR6 Source Port Mode     | Shows if the switch only forwards multicast streams which the source port has dynamically joined or always forwards multicast streams   |
| Domain                    | An independent multicast domain.  |
| MVR6 Config Status        | Shows if MVR6 is globally enabled on the switch.  |
| MVR6 Running Status       | 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 <code>mvr6 type</code> command.) |
| MVR6 Multicast VLAN       | Shows the VLAN used to transport all MVR6 multicast traffic.  |
| MVR6 Upstream Source IP   | The source IP address assigned to all upstream control packets.   |

**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.
-----
rd                      ff01::fe              ff01::ff
Console#

```

**show mvr6 interface** This command shows MVR6 configuration settings for interfaces attached to the MVR VLAN.

### Syntax

**show mvr6 [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

### 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 138: show mvr6 interface - display description**

| Field                | Description  |
|----------------------|--|
| Port                 | Shows interfaces attached to the MVR.  |
| Type                 | Shows the MVR6 port type.  |
| Status               | 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. |
| Immediate            | Shows if immediate leave is enabled or disabled.   |
| Static Group Address | Shows any static MVR6 group assigned to an interface, and the receiver VLAN.   |

**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).

Group Address          VLAN Port          Up time          Expire Count
-----
ff05::101              2                  00:00:00:19     2 (P)
                       2 Eth1/ 2 (S)
                       1 Eth1/ 4 (R)
                       0 (H)

Console#

```

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).

Group Address          VLAN Port          Up time          Expire Count
-----
ff05::101              2                  00:00:03:18     2 (P)
                       2 Eth1/ 2 (S)
                       1 Eth1/ 4 (R)
                       0 (H)

Console#

```

**Table 139: show mvr6 members - display description**

| Field         | Description   |
|---------------|---|
| Group Address | Multicast group address.  |
| VLAN          | VLAN to which this address is forwarded.                                  |
| Port          | Port to which this address is forwarded.                                  |
| Up time       | Time that this multicast group has been known.                            |
| Expire        | The time until this entry expires.  |
| Count         | The number of times this address has been learned by MVR6 (MLD-snooping). |

**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 MVR6 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 | summary {ethernet *interface* | mvr-vlan | port-channel *channel-id*}}

*domain-id* - An independent multicast domain. (Range: 1-5)

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

**vlan** *vlan-id* - VLAN ID (Range: 1-4094)

**query** - Displays MVR6 query-related statistics.

**summary** - Displays MVR6 summary information.

**mvr vlan** - Displays summary statistics for the MVR6 VLAN.

### 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 140: show mvr6 statistics input - display description**

| Field         | Description   |
|---------------|---|
| Interface     | Shows interfaces attached to the MVR6.  |
| Report        | The number of IGMP membership reports received on this interface.   |
| Leave         | The number of leave messages received on this interface.  |
| G Query       | The number of general query messages received on this interface.  |
| G(-S)-S Query | The number of group specific or group-and-source specific query messages received on this interface.  |
| Drop          | 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 |
| Join Succ     | The number of times a multicast group was successfully joined.  |
| Group         | The number of MVR6 groups active on this interface.   |

The following shows MVR6 protocol-related statistics sent:

```

Console#show mvr6 domain 1 statistics output
MVR6 Domain 1, MVR6 VLAN 2:
Output Statistics:
Interface Report    Done     G Query  G(-S)-S Query Drop    Group
-----
Eth 1/ 1           12         0         1         0         0         0
Eth 1/ 3            5         1         4         1         0         0
DVLAN  1            7         2         3         0         0         0
    
```

```
MVLAN 2 7 2 3 0 0 0
Console#
```

**Table 141: show mvr6 statistics output - display description**

| Field         | Description  |
|---------------|--|
| Interface     | Shows interfaces attached to the MVR.  |
| Report        | The number of IGMP membership reports sent from this interface.                                    |
| Leave         | The number of leave messages sent from this interface.   |
| G Query       | The number of general query messages sent from this interface.                                     |
| G(-S)-S Query | The number of group specific or group-and-source specific query messages sent from this interface. |
| Group         | The number of MVR groups active on this interface.   |

The following shows MVR6 query-related statistics:

```
Console#show mvr6 domain 1 statistics query
Other Querier Address : fe80::2e0:cff: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#
```

**Table 142: show mvr6 statistics query - display description**

| Field                     | Description   |
|---------------------------|---|
| Other Querier Address     | The IPv6 address of the querier on this interface.            |
| Other Querier Uptime      | Other querier's time up.                                      |
| Other Querier Expire Time | The time after which this querier is assumed to have expired. |
| Self Querier Address      | This querier's IPv6 address.                                  |
| Self Querier Uptime       | This querier's time up.                                       |
| Self Querier Expire Time  | This querier's expire time.                                   |
| General Query Received    | The number of general queries received on this interface.     |
| General Query Sent        | The number of general queries sent from this interface.       |
| Specific Query Received   | The number of specific queries received on this interface.    |
| Specific Query Sent       | The number of specific queries sent from this interface.      |

The following shows MVR6 summary statistics for an interface:

```

Console#show mvr6 domain 1 statistics summary interface ethernet 1/1
Domain 1:
Number of Groups: 0
Querier:          :          Report & Leave:  :
Transmit         :          Transmit         :
  General        : 0          Report         : 7
  Group Specific : 0          Leave          : 4
Received         :          Recieved         :
  General        : 0          Report         : 0
  Group Specific : 0          Leave          : 0
                                   Join Success  : 0
                                   Filter Drop   : 0
                                   Source Port Drop: 0
                                   Others Drop   : 0

Console#

```

**Table 143: show mvr6 statistics summary interface - display description**

| Field            | Description   |
|------------------|---|
| Domain           | An independent multicast domain.                            |
| Number of Groups | Number of groups learned on this port.                      |
| Querier          |   |
| Transmit         |   |
| General          | Number of general queries transmitted.                      |
| Group Specific   | Number of group specific queries transmitted.               |
| Received         |   |
| General          | Number of general queries received.                         |
| Group Specific   | Number of group specific queries received.                  |
| Report & Leave   |   |
| Transmit         |   |
| Report           | Number of transmitted reports.                              |
| Leave            | Number of transmitted leaves.                               |
| Received         |   |
| Report           | Number of reports received.                                 |
| Leave            | Number of leaves received.                                  |
| Join Success     | Number of join reports processed successfully.              |
| Filter Drop      | Number of report/leave messages dropped by IGMP filter.     |
| Source Port Drop | Number of report/leave messages dropped by MVR source port. |
| Others Drop      | Number of report/leave messages dropped for other reasons.  |

The following shows MVR6 summary statistics for the MVR6 VLAN:

```

Console#show mvr6 domain 1 statistics summary interface mvr-vlan
Domain 1:
Number of Groups: 0
Querier:          :                               Report & Leave:   :
  Other Addr      : None
                                     Host Addr       : None
  Other Expire    : 0(m): 0(s)                   Unsolicit Expire : 0 sec
  Other Uptime    : 0(h): 0(m): 0(s)
  Self Addr       : None
  Self Expire     : 0(m): 0(s)
  Self Uptime     : 0(h): 0(m): 0(s)
  Transmit       :                               Transmit       :
    General       : 0                               Report         : 0
    Group Specific : 0                               Leave          : 0
  Recieved       :                               Recieved       :
    General       : 0                               Report         : 0
    Group Specific : 0                               Leave          : 0
                                     join Success    : 0
                                     Filter Drop     : 0
                                     Source Port Drop : 0
                                     Others Drop      : 0
Console#

```

**Table 144: show mvr6 statistics summary interface mvr vlan - description**

| Field            | Description  |
|------------------|--|
| Domain           | An independent multicast domain.                                       |
| Number of Groups | Number of groups learned on this port.                                 |
| Querier          |  |
| Other Addr       | Other IGMP querier's IP address.                                       |
| Other Expire     | Other querier's expire time.   |
| Other Uptime     | Other querier's time up.   |
| Self Addr        | This querier's IP address.   |
| Self Expire      | This querier's expire time.  |
| Self Uptime      | This querier's time up.  |
| Transmit         |  |
| General          | Number of general queries sent from receiver port.                     |
| Group Specific   | Number of group specific queries sent from receiver port.              |
| Received         |  |
| General          | Number of general queries received.                                    |
| Group Specific   | Number of group specific queries received.                             |
| Report & Leave   |  |
| Host Addr        | Source IP address used to send report/leave messages from source port. |
| Unsolicit Expire | Expiration time for unsolicit reports sent out from source port        |

**Table 144: show mvr6 statistics summary interface mvr vlan - description**

| Field            | Description   |
|------------------|---|
| Transmit         |   |
| Report           | Number of reports sent out from source port.                |
| Leave            | Number of leaves sent out from source port.                 |
| Received         | Field header  |
| Report           | Number of reports received.                                 |
| Leave            | Number of leaves received.                                  |
| Join Success     | Number of join reports processed successfully.              |
| Filter Drop      | Number of report/leave messages dropped by IGMP filter.     |
| Source Port Drop | Number of report/leave messages dropped by MVR source port. |
| Others Drop      | Number of report/leave messages dropped for other reasons.  |



## 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 145: LLDP Commands**

| Command   | Function   | Mode |
|---|--|------|
| <code>lldp</code>                                 | Enables LLDP globally on the switch  | GC   |
| <code>lldp holdtime-multiplier</code>             | Configures the time-to-live (TTL) value sent in LLDP advertisements  | GC   |
| <code>lldp med-fast-start-count</code>            | Configures how many medFastStart packets are transmitted   | GC   |
| <code>lldp notification-interval</code>           | Configures the allowed interval for sending SNMP notifications about LLDP changes  | GC   |
| <code>lldp refresh-interval</code>                | Configures the periodic transmit interval for LLDP advertisements  | GC   |
| <code>lldp reinit-delay</code>                    | Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down                | GC   |
| <code>lldp tx-delay</code>                        | Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables | GC   |
| <code>lldp admin-status</code>                    | Enables LLDP transmit, receive, or transmit and receive mode on the specified port   | IC   |
| <code>lldp basic-tlv management-ip-address</code> | Configures an LLDP-enabled port to advertise the management address for this device  | IC   |
| <code>lldp basic-tlv port-description</code>      | Configures an LLDP-enabled port to advertise its port description  | IC   |
| <code>lldp basic-tlv system-capabilities</code>   | Configures an LLDP-enabled port to advertise its system capabilities   | IC   |

Table 145: LLDP Commands (Continued)

| Command  | Function  | Mode |
|--|---|------|
| <code>lldp basic-tlv system-description</code> | Configures an LLDP-enabled port to advertise the system description                       | IC   |
| <code>lldp basic-tlv system-name</code>        | Configures an LLDP-enabled port to advertise its system name                              | IC   |
| <code>lldp dot1-tlv proto-ident*</code>        | Configures an LLDP-enabled port to advertise the supported protocols                      | IC   |
| <code>lldp dot1-tlv proto-vid*</code>          | Configures an LLDP-enabled port to advertise port-based protocol related VLAN information | IC   |
| <code>lldp dot1-tlv pvid*</code>               | Configures an LLDP-enabled port to advertise its default VLAN ID                          | IC   |
| <code>lldp dot1-tlv vlan-name*</code>          | Configures an LLDP-enabled port to advertise its VLAN name                                | IC   |
| <code>lldp dot3-tlv link-agg</code>            | Configures an LLDP-enabled port to advertise its link aggregation capabilities            | IC   |
| <code>lldp dot3-tlv mac-phy</code>             | Configures an LLDP-enabled port to advertise its MAC and physical layer specifications    | IC   |
| <code>lldp dot3-tlv max-frame</code>           | Configures an LLDP-enabled port to advertise its maximum frame size                       | IC   |
| <code>lldp med-location civic-addr</code>      | Configures an LLDP-MED-enabled port to advertise its location identification details      | IC   |
| <code>lldp med-notification</code>             | Enables the transmission of SNMP trap notifications about LLDP-MED changes                | IC   |
| <code>lldp med-tlv inventory</code>            | Configures an LLDP-MED-enabled port to advertise its inventory identification details     | IC   |
| <code>lldp med-tlv location</code>             | Configures an LLDP-MED-enabled port to advertise its location identification details      | IC   |
| <code>lldp med-tlv med-cap</code>              | Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities   | IC   |
| <code>lldp med-tlv network-policy</code>       | Configures an LLDP-MED-enabled port to advertise its network policy configuration         | IC   |
| <code>lldp notification</code>                 | Enables the transmission of SNMP trap notifications about LLDP changes                    | IC   |
| <code>show lldp config</code>                  | Shows LLDP configuration settings for all ports   | PE   |
| <code>show lldp info local-device</code>       | Shows LLDP global and interface-specific configuration settings for this device           | PE   |
| <code>show lldp info remote-device</code>      | Shows LLDP global and interface-specific configuration settings for remote devices        | PE   |
| <code>show lldp info statistics</code>         | Shows statistical counters for all LLDP-enabled interfaces                                | PE   |

\* 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

**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

```
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

**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 `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` 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:  
 $(4 * \text{tx-delay}) \leq \text{refresh-interval}$

**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**

**rx-only** - Only receive LLDP PDUs.

**tx-only** - Only transmit LLDP PDUs.

**tx-rx** - Both transmit and receive LLDP Protocol Data Units (PDUs).

#### 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

**[no] 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

```
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

```
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

**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(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(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 port-based protocol VLANs configured on this interface (see [“Configuring Protocol-based VLANs” on page 550](#)).

**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 531](#) and [“protocol-vlan protocol-group \(Configuring Interfaces\)” on page 552](#).

**Example**

```
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**

```
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)#
```

**lldp 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 112](#) 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)#
```

**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 146: LLDP MED Location CA Types**

| CA Type | Description                                     | CA Value Example |
|---------|---|------------------|
| 1       | National subdivisions (state, canton, province) | California       |
| 2       | County, parish                                  | Orange           |
| 3       | City, township                                  | Irvine           |
| 4       | City division, borough, city district           | West Irvine      |
| 5       | Neighborhood, block                             | Riverside        |

Table 146: LLDP MED Location CA Types (Continued)

| CA Type | Description                                   | CA Value Example |
|---------|---|------------------|
| 6       | Group of streets below the neighborhood level | Exchange         |
| 18      | Street suffix or type                         | Avenue           |
| 19      | House number                                  | 320              |
| 20      | House number suffix                           | A                |
| 21      | Landmark or vanity address                    | Tech Center      |
| 26      | Unit (apartment, suite)                       | Apt 519          |
| 27      | Floor   | 5                |
| 28      | Room  | 509B             |

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(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 6 Exchange
Console(config-if)#lldp med-location civic-addr 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)#

```

**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

**[no] 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 `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` 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 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**

```

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: 1-12)

**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
                              : link-agg
                              : max-frame

MED Notification Status      : Enabled
MED Enabled TLVs Advertised  : med-cap
                              : network-policy
                              : location
                              : inventory

MED Location Identification
Location Data Format : Civic Address LCI
Civic Address Status : Enabled
Country Name       : US
What               : 2
CA-Type           : 1
CA-Value          : Alabama
CA-Type           : 2
CA-Value          : Tuscaloosa

Console#

```

**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: 1-12)

**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            : 70-72-CF-32-DD-CD
System Name           :
System Description    : ECS4810-12M
System Capabilities Support : Bridge
System Capabilities Enabled : Bridge
Management Address   : 192.168.0.2 (IPv4)

LLDP Local Port Information
-----
Port      PortID Type      PortID      Port Description
-----
Eth 1/1  MAC Address    00-12-CF-DA-FC-E9 Ethernet Port on unit 0, port 1
Eth 1/2  MAC Address    00-12-CF-DA-FC-EA Ethernet Port on unit 0, port 2
Eth 1/3  MAC Address    00-12-CF-DA-FC-EB Ethernet Port on unit 0, port 3
Eth 1/4  MAC Address    00-12-CF-DA-FC-EC Ethernet Port on unit 0, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1
LLDP Local Port Information Detail
Port           : Eth 1/1
Port ID Type   : MAC Address
Port ID        : 70-72-CF-32-DD-CE
Port Description : Ethernet Port on unit 1, port 1
MED Capability : LLDP-MED Capabilities
                Network Policy
                Location Identification
                Inventory

Console#

```

**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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### 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 LLDP-MED Capability” and other related fields.

```

Console#show lldp info remote-device
LLDP Remote Devices Information
Interface Chassis ID      Port ID      System Name
-----
Eth 1/1    00-E0-0C-00-00-FD 00-E0-0C-00-01-02

```

```

Console#show lldp info remote-device detail ethernet 1/1
LLDP Remote Devices Information Detail
-----

```

```

Index          : 4
Chassis Type   : MAC Address
Chassis ID     : 70-72-CF-5B-DA-D4
Port ID Type   : MAC Address
Port ID        : 70-72-CF-5B-DA-D5
Time To Live   : 120 seconds
Port Description : Ethernet Port on unit 1, port 1
System Description : ECS4810-12M
System Capabilities : Bridge
Enabled Capabilities : Bridge

```

```
Management Address : 192.168.0.3 (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

```

```
Link Aggregation
```

```

Link Aggregation Capable : Yes
Link Aggregation Enable  : No
Link Aggregation Port ID : 0

```

```
Max Frame Size : 1522
```

```
Console#
```

The following example shows information which is displayed for end-node device which advertises LLDP-MED TLVs.

```

...
LLDP-MED Capability :
Device Class          : Network Connectivity
Supported Capabilities : LLDP-MED Capabilities
                        Network Policy
                        Location Identification
                        Extended Power via MDI - PSE

```

```

Current Capabilities          : LLDP-MED Capabilities
                              : Location Identification
                              : Extended Power via MDI - PSE
                              : Inventory

Location Identification :
  Location Data Format      : Civic Address LCI
  Country Name            : TW
  What                    : 2
Extended Power via MDI :
  Power Type              : PSE
  Power Source            : Unknown
  Power Priority           : Unknown
  Power Value             : 0 Watts
Inventory                :
  Hardware Revision       : R0A
  Firmware Revision       : 1.2.6.0
  Software Revision       : 1.2.6.0
  Serial Number           : S123456
  Manufacture Name        : Prye
  Model Name              : VP101
  Asset ID                 : 340937

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: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### Command Mode

Privileged Exec

### Example

```

Console#show lldp info statistics
LLDP Global Statistics
Neighbor Entries List Last Updated : 12591 seconds
New Neighbor Entries Count         : 4
Neighbor Entries Deleted Count     : 2
Neighbor Entries Dropped Count     : 0
Neighbor Entries Ageout Count      : 0

```

```
LLDP Port Statistics
```

| Port    | NumFramesRecvd | NumFramesSent | NumFramesDiscarded |
|---------|----------------|---------------|--------------------|
| Eth 1/1 | 235            | 234           | 0                  |
| Eth 1/2 | 0              | 428           | 0                  |
| Eth 1/3 | 0              | 0             | 0                  |
| Eth 1/4 | 8              | 9             | 0                  |
| Eth 1/5 | 0              | 0             | 0                  |

```
:  
Console#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 : 238  
Frames Sent     : 238  
TLVs Unrecognized : 0  
TLVs Discarded  : 0  
Neighbor Ageouts : 0  
Neighbor Ageouts : 0
```

```
Console#
```

---

## CFM Commands

Connectivity Fault Management (CFM) is an OAM protocol that includes proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between provider edge devices or between customer edge devices.

CFM is implemented as a service level protocol based on service instances which encompass only that portion of the metropolitan area network supporting a specific customer. CFM can also provide controlled management access to a hierarchy of maintenance domains (such as the customer, service provider, and equipment operator).

The following list of commands support functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also provides commands for fault detection through continuity check messages for all known maintenance points, and cross-check messages for statically configured maintenance points located on other devices. Fault verification is supported through loop back messages, and fault isolation through link trace messages. Fault notification is also provided by SNMP alarms which are automatically generated by maintenance points when connectivity faults or configuration errors are detected in the local maintenance domain.

**Table 147: CFM Commands**

| Command                                      | Function   | Mode |
|--|--|------|
| <i>Defining CFM Structures</i>               |  |      |
| <code>ethernet cfm ais level</code>          | Configures the maintenance level at which Alarm Indication Signal information will be sent   | GC   |
| <code>ethernet cfm ais ma</code>             | Enables the MEPs within the specified MA to send frames with AIS information   | GC   |
| <code>ethernet cfm ais period</code>         | Configures the interval at which AIS information is sent   | GC   |
| <code>ethernet cfm ais suppress alarm</code> | Suppresses AIS messages following the detection of defect conditions   | GC   |
| <code>ethernet cfm domain</code>             | Defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode; also specifies the MIP creation method for MAs within this domain            | GC   |
| <code>ethernet cfm enable</code>             | Enables CFM processing globally on the switch  | GC   |
| <code>ma index name</code>                   | Creates a maintenance association within the current maintenance domain, maps it to a customer service instance, and sets the manner in which MIPs are created for this service instance | CFM  |

Table 147: CFM Commands (Continued)

| Command  | Function   | Mode |
|--|--|------|
| <code>ma index name-format</code>                                  | Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format                                    | CFM  |
| <code>ethernet cfm mep</code>                                      | Sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages               | IC   |
| <code>ethernet cfm port-enable</code>                              | Enables CFM processing on an interface   | IC   |
| <code>clear ethernet cfm ais mpid</code>                           | Clears AIS defect information for the specified MEP  | PE   |
| <code>show ethernet cfm configuration</code>                       | Displays CFM configuration settings, including global settings, SNMP traps, and interface settings   | PE   |
| <code>show ethernet cfm md</code>                                  | Displays configured maintenance domains  | PE   |
| <code>show ethernet cfm ma</code>                                  | Displays configured maintenance associations   | PE   |
| <code>show ethernet cfm maintenance-points local</code>            | Displays maintenance points configured on this device  | PE   |
| <code>show ethernet cfm maintenance-points local detail mep</code> | Displays detailed CFM information about a specified local MEP in the continuity check database   | PE   |
| <code>show ethernet cfm maintenance-points remote detail</code>    | Displays detailed CFM information about a specified remote MEP in the continuity check database  | PE   |
| <i>Continuity Check Operations</i>                                 |  |      |
| <code>ethernet cfm cc ma interval</code>                           | Sets the transmission delay between continuity check messages  | GC   |
| <code>ethernet cfm cc enable</code>                                | Enables transmission of continuity check messages within a specified maintenance association   | GC   |
| <code>snmp-server enable traps ethernet cfm cc</code>              | Enables SNMP traps for CFM continuity check events   | GC   |
| <code>mep archive-hold-time</code>                                 | Sets the time that data from a missing MEP is kept in the continuity check database before being purged  | CFM  |
| <code>clear ethernet cfm maintenance-points remote</code>          | Clears the contents of the continuity check database   | PE   |
| <code>clear ethernet cfm errors</code>                             | Clears continuity check errors logged for the specified maintenance domain and maintenance level   | PE   |
| <code>show ethernet cfm errors</code>                              | Displays CFM continuity check errors logged on this device   | PE   |
| <i>Cross Check Operations</i>                                      |  |      |
| <code>ethernet cfm mep crosscheck start-delay</code>               | Sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation  | GC   |
| <code>snmp-server enable traps ethernet cfm crosscheck</code>      | Enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages | GC   |
| <code>mep crosscheck mpid</code>                                   | Statically defines a remote MEP in a maintenance association   | CFM  |

Table 147: CFM Commands (Continued)

| Command   | Function  | Mode |
|---|---|------|
| <code>ethernet cfm mep crosscheck</code>                            | Enables cross-checking between the list of configured remote MEPs within a maintenance association and MEPs learned through continuity check messages | PE   |
| <code>show ethernet cfm maintenance-points remote crosscheck</code> | Displays information about remote maintenance points configured statically in a cross-check list  | PE   |
| <i>Link Trace Operations</i>  |   |      |
| <code>ethernet cfm linktrace cache</code>                           | Enables caching of CFM data learned through link trace messages   | GC   |
| <code>ethernet cfm linktrace cache hold-time</code>                 | Sets the hold time for CFM link trace cache entries   | GC   |
| <code>ethernet cfm linktrace cache size</code>                      | Sets the maximum size for the link trace cache  | GC   |
| <code>ethernet cfm linktrace</code>                                 | Sends CFM link trace messages to the MAC address for a MEP  | PE   |
| <code>clear ethernet cfm linktrace-cache</code>                     | Clears link trace messages logged on this device  | PE   |
| <code>show ethernet cfm linktrace-cache</code>                      | Displays the contents of the link trace cache   | PE   |
| <i>Loopback Operations</i>  |   |      |
| <code>ethernet cfm loopback</code>                                  | Sends CFM loopback messages to a MAC address for a MEP or MIP   | PE   |
| <i>Fault Generator Operations</i>                                   |   |      |
| <code>mep fault-notify alarm-time</code>                            | Sets the time a defect must exist before a fault alarm is issued  | CFM  |
| <code>mep fault-notify lowest-priority</code>                       | Sets the lowest priority defect that is allowed to generate a fault alarm   | CFM  |
| <code>mep fault-notify reset-time</code>                            | Configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued                               | CFM  |
| <code>show ethernet cfm fault-notify-generator</code>               | Displays configuration settings for the fault notification generator  | PE   |
| <i>Delay Measure Operations</i>                                     |   |      |
| <code>ethernet cfm delay-measure two-way</code>                     | Sends periodic delay-measure requests to a specified MEP within a maintenance association   | PE   |

*Basic Configuration Steps for CFM*

1. Configure the maintenance domains with the `ethernet cfm domain` command.
2. Configure the maintenance associations with the `ma index name` command.
3. Configure the local maintenance end points (MEPs) which will serve as the domain service access points for the specified maintenance association using the `ethernet cfm mep` command.

4. Enter a static list of MEPs assigned to other devices within the same maintenance association using the `mep crosscheck mpid` command. This allows CFM to automatically verify the functionality of these remote end points by cross-checking the static list configured on this device against information learned through continuity check messages.
5. Enable CFM globally on the switch with the `ethernet cfm enable` command.
6. Enable CFM on the local MEPs with the `ethernet cfm port-enable` command.
7. Enable continuity check operations with the `ethernet cfm cc enable` command.
8. Enable cross-check operations with the `ethernet cfm mep crosscheck` command.

Other configuration changes may be required for your particular environment, such as adjusting the interval at which continuity check messages are sent (page 755), or setting the start-up delay for the cross-check operation (page 761). You can also enable SNMP traps for events discovered by continuity check messages (page 757) or cross-check messages (page 761).

## Defining CFM Structures

**ethernet cfm ais level** This command configures the maintenance level at which Alarm Indication Signal (AIS) information will be sent within the specified MA. Use the **no** form restore the default setting.

### Syntax

**ethernet cfm ais level** *level-id* **md** *domain-name* **ma** *ma-name*

**no ethernet cfm ais level md** *domain-name* **ma** *ma-name*

*level-id* – Maintenance level at which AIS information will be sent.  
(Range: 0-7)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

Level 0

### Command Mode

Global Configuration

### Command Usage

The configured AIS level must be higher than the maintenance level of the domain containing the specified MA.

### Example

This example sets the maintenance level for sending AIS messages within the specified MA.

```
Console(config)#ethernet cfm ais level 4 md voip ma rd
Console(config)#
```

**ethernet cfm ais ma** This command enables the MEPs within the specified MA to send frames with AIS information following detection of defect conditions. Use the **no** form to disable this feature.

### Syntax

**[no] ethernet cfm ais md** *domain-name* **ma** *ma-name*

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name.<sup>14</sup> (Range: 1-43 alphanumeric characters)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ Each MA name must be unique within the CFM domain.
- ◆ Frames with AIS information can be issued at the client's maintenance level by a MEP upon detecting defect conditions. For example, defect conditions may include:
  - Signal failure conditions if continuity checks are enabled.
  - AIS condition or LCK condition if continuity checks are disabled.
- ◆ A MEP continues to transmit periodic frames with AIS information until the defect condition is removed.

### Example

This example enables the MEPs within the specified MA to send frames with AIS information.

```
Console(config)#ethernet cfm ais md voip ma rd
Console(config)#
```

14. The total length of the MD name and MA name cannot exceed 44 characters.

**ethernet cfm ais period** This command configures the interval at which AIS information is sent. Use the **no** form to restore the default setting.

#### Syntax

**ethernet cfm ais period** *period* **md** *domain-name* **ma** *ma-name*

**no ethernet cfm ais period md** *domain-name* **ma** *ma-name*

*period* – The interval at which AIS information is sent.  
(Options: 1 second, 60 seconds)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

#### Default Setting

1 second

#### Command Mode

Global Configuration

#### Example

This example sets the interval for sending frames with AIS information at 60 seconds.

```
Console(config)#ethernet cfm ais period 60 md voip ma rd
Console(config)#
```

**ethernet cfm ais suppress alarm** This command suppresses sending frames containing AIS information following the detection of defect conditions. Use the **no** form to restore the default setting.

#### Syntax

**[no] ethernet cfm ais suppress alarm md** *domain-name* **ma** *ma-name*

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

#### Default Setting

Suppression is disabled

#### Command Mode

Global Configuration

#### Command Usage

- ◆ For multipoint connectivity, a MEP cannot determine the specific maintenance level entity that has encountered defect conditions upon receiving a frame

with AIS information. More importantly, it cannot determine the associated subset of its peer MEPs for which it should suppress alarms since the received AIS information does not contain that information. Therefore, upon reception of a frame with AIS information, the MEP will suppress alarms for all peer MEPs whether there is still connectivity or not.

- ◆ However, for a point-to-point connection, a MEP has only a single peer MEP for which to suppress alarms when it receives frames with AIS information.
- ◆ If suppression is enabled by this command, upon receiving a frame with AIS information, a MEP detects an AIS condition and suppresses loss of continuity alarms associated with all its peer MEPs. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of AIS messages.

### Example

This example suppresses sending frames with AIS information.

```
Console(config)#ethernet cfm ais suppress alarm md voip ma rd
Console(config)#
```

**ethernet cfm domain** This command defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode. Use the **no** form to delete a CFM maintenance domain.

### Syntax

**ethernet cfm domain index** *index* **name** *domain-name* **level** *level-id* [**mip-creation** *type*]

**no ethernet cfm domain index** *index*

*index* – Domain index. (Range: 1-65535)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Authorized maintenance level for this domain. (Range: 0-7)

*type* – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:

**default** – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.

**explicit** – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

**none** – No MIP can be created for any MA configured in this domain.

### Default Setting

No maintenance domains are configured.  
No MIPs are created for any MA in the specified domain.

### Command Mode

Global Configuration

### Command Usage

- ◆ A domain can only be configured with one name.
- ◆ Where domains are nested, an upper-level hierarchical domain must have a higher maintenance level than the ones it encompasses. The higher to lower level domain types commonly include entities such as customer, service provider, and operator.
- ◆ More than one domain can be configured at the same maintenance level, but a single domain can only be configured with one maintenance level.
- ◆ If MEPs or MAs are configured for a domain using the `ethernet cfm mep` command or `ma index name` command, they must first be removed before you can remove the domain.
- ◆ Maintenance domains are designed to provide a transparent method of verifying and resolving connectivity problems for end-to-end connections. By default, these connections run between the domain service access points (DSAPs) within each MA defined for a domain, and are manually configured using the `ethernet cfm mep` command.

In contrast, MIPs are interconnection points that make up all possible paths between the DSAPs within an MA. MIPs are automatically generated by the CFM protocol when the `mip-creation` option in this command is set to "default" or "explicit," and the MIP creation state machine is invoked (as defined in IEEE 802.1ag). The default option allows MIPs to be created for all interconnection points within an MA, regardless of the domain's level in the maintenance hierarchy (e.g., customer, provider, or operator). While the explicit option only generates MIPs within an MA if its associated domain is not at the bottom of the maintenance hierarchy. This option is used to hide the structure of network at the lowest domain level.

The diagnostic functions provided by CFM can be used to detect connectivity failures between any pair of MEPs in an MA. Using MIPs allows these failures to be isolated to smaller segments of the network.

Allowing the CFM to generate MIPs exposes more of the network structure to users at higher domain levels, but can speed up the process of fault detection and recovery. This trade-off should be carefully considered when designing a CFM maintenance structure.

Also note that while MEPs are active agents which can initiate consistency check messages (CCMs), transmit loop back or link trace messages, and maintain the local CCM database. MIPs, on the other hand are passive agents

which can only validate received CFM messages, and respond to loop back and link trace messages.

The MIP creation method defined by the `ma index name` command takes precedence over the method defined by this command.

### Example

This example creates a maintenance domain set to maintenance level 3, and enters CFM configuration mode for this domain.

```
Console(config)#ethernet cfm domain index 1 name voip level 3 mip-creation  
explicit  
Console(config-ether-cfm)#
```

### Related Commands

[ma index name \(744\)](#)

**ethernet cfm enable** This command enables CFM processing globally on the switch. Use the **no** form to disable CFM processing globally.

### Syntax

**[no] ethernet cfm enable**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to globally enabling CFM processing with this command. Specifically, the maintenance domains, maintenance associations, and MEPs should be configured on each participating bridge.
- ◆ When CFM is enabled, hardware resources are allocated for CFM processing.

### Example

This example enables CFM globally on the switch.

```
Console(config)#ethernet cfm enable  
Console(config)#
```

**ma index name** This command creates a maintenance association (MA) within the current maintenance domain, maps it to a customer service instance (S-VLAN), and sets the manner in which MIPs are created for this service instance. Use the **no** form with the **vlan** keyword to remove the S-VLAN from the specified MA. Or use the **no** form with only the **index** keyword to remove the MA from the current domain.

### Syntax

**ma index** *index name* *ma-name* [**vlan** *vlan-id* [**mip-creation** *type*]]

**no ma index** *index* [**vlan** *vlan-id*]

*index* – MA identifier. (Range: 1-2147483647)

*vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

*vlan-id* - Service VLAN ID. (Range: 1-4093)

*type* – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:

**default** – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.

**explicit** – MIPs can be created this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

**none** – No MIP can be created for this MA.

### Default Setting

10 seconds

### Command Mode

CFM Domain Configuration

### Command Usage

- ◆ The maintenance domain used to enter CFM domain configuration mode, the MA name and VLAN identifier specified by this command, and the DSAPs configured with the [mep crosscheck mpid](#) command create a unique service instance for each customer.
- ◆ If only the MA index and name are entered for this command, the MA will be recorded in the domain database, but will not function. No MEPs can be created until the MA is associated with a service VLAN.
- ◆ Note that multiple domains at the same maintenance level (see the [ethernet cfm domain](#) command) cannot have an MA on the same VLAN. Also, each MA name must be unique within the CFM-managed network.
- ◆ The first VLAN entered in the list by this command is the primary VLAN, and is the VLAN on which all CFM functions are executed.

- ◆ Before removing an MA, first remove all the MEPs configured for it (see the [mep crosscheck mpid](#) command).
- ◆ If the MIP creation method is not defined by this command, the creation method defined by the [ethernet cfm domain](#) command is applied to this MA. For a detailed description of the MIP types, refer to the Command Usage section under the [ethernet cfm domain](#) command.

### Example

This example creates a maintenance association, binds it to VLAN 1, and allows MIPs to be created within this MA using the default method.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1 mip-creation default
Console(config-ether-cfm)#
```

**ma index name-format** This command specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format. Use the **no** form to restore the default setting.

### Syntax

**ma index** *index* **name-format** {**character-string** | **icc-based**}

**no ma index** *index* **name-format**

*index* – MA identifier. (Range: 1-2147483647)

**character-string** – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.

**icc-based** – ITU-T SG13/SG15 Y.1731 defined ICC based format.

### Default Setting

character-string

### Command Mode

CFM Domain Configuration

### Example

This example specifies the name format as character string.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name-format character-string
Console(config-ether-cfm)#
```

**ethernet cfm mep** This command sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages. Use the **no** form to delete a MEP.

### Syntax

**ethernet cfm mep mpid** *mpid* **md** *domain-name* **ma** *ma-name* [**up**]

**no ethernet cfm mep mpid** *mpid* **ma** *ma-name*

*mpid* – Maintenance end point identifier. (Range: 1-8191)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

**up** – Indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the **up** keyword is not included in this command, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.

### Default Setting

No MEPs are configured.  
The MEP faces outward (down).

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured (using the **ethernet cfm domain** command), (2) maintenance association within the domain (using the **ma index name** command), and (3) finally the MEP using this command.
- ◆ An interface may belong to more than one domain. This command can be used to configure an interface as a MEP for different MAs in different domains.
- ◆ To change the MEP's MA or the direction it faces, first delete the MEP, and then create a new one.

### Example

This example sets port 1 as a DSAP for the specified maintenance association.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm mep mpid 1 md voip ma rd
Console(config-if)#
```

**ethernet cfm port-enable** This command enables CFM processing on an interface. Use the **no** form to disable CFM processing on an interface.

### Syntax

**[no] ethernet cfm port-enable**

### Default Setting

Enabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- ◆ An interface must be enabled before a MEP can be created with the **ethernet cfm mep** command.
- ◆ If a MEP has been configured on an interface with the **ethernet cfm mep** command, it must first be deleted before CFM can be disabled on that interface.
- ◆ When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

### Example

This example enables CFM on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm port-enable
Console(config-if)#
```

**clear ethernet cfm ais mpid** This command clears AIS defect information for the specified MEP.

### Syntax

**clear ethernet cfm ais mpid mpid md domain-name ma ma-name**

*mpid* – Maintenance end point identifier. (Range: 1-8191)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

This command can be used to clear AIS defect entries if a MEP does not exit the AIS state when all errors are resolved.

### Example

This example clears AIS defect entries on port 1.

```
Console#clear ethernet cfm ais mpid 1 md voip ma rd
Console(config)#
```

**show ethernet cfm configuration** This command displays CFM configuration settings, including global settings, SNMP traps, and interface settings.

### Syntax

**show ethernet cfm configuration** {**global** | **traps** | **interface** *interface*}

**global** – Displays global settings including CFM global status, cross-check start delay, and link trace parameters.

**traps** – Displays the status of all continuity check and cross-check traps.

*interface* – Displays CFM status for the specified interface.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows the global settings for CFM.

```
Console#show ethernet cfm configuration global
CFM Global Status      : Enabled
Crosscheck Start Delay : 10 seconds
Linktrace Cache Status : Enabled
Linktrace Cache Hold Time : 100 minutes
Linktrace Cache Size   : 100 entries
Console#
```

This example shows the configuration status for continuity check and cross-check traps.

```

Console#show ethernet cfm configuration traps
CC MEP Up Trap           :Disabled
CC MEP Down Trap        :Disabled
CC Configure Trap       :Disabled
CC Loop Trap            :Disabled
Cross Check MEP Unknown Trap :Disabled
Cross Check MEP Missing Trap :Disabled
Cross Check MA Up       :Disabled
Console#

```

**Table 148: show ethernet cfm configuration traps - display description**

| Field                        | Description   |
|------------------------------|---|
| CC MEP Up Trap               | Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database.                          |
| CC Mep Down Trap             | Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.  |
| CC Configure Trap            | Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.   |
| CC Loop Trap                 | Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.  |
| Cross Check MEP Unknown Trap | A CCM is received from a MEP that has not been configured as a DSAP (see the <a href="#">ethernet cfm mep</a> command), manually configured as a remote MEP (see the <a href="#">mep crosscheck mpid</a> command), nor learned through previous CCM messages. |
| Cross Check MEP Missing Trap | This device failed to receive three consecutive CCMs from another MEP in the same MA.   |
| Cross Check MA Up            | Generates a trap when all remote MEPs belonging to an MA come up.   |

This example shows the CFM status for port 1.

```

Console#show ethernet cfm configuration interface ethernet 1/1
Ethernet 1/1 CFM Status:Enabled
Console#

```

**show ethernet cfm md** This command displays the configured maintenance domains.

### Syntax

**show ethernet cfm md** [**level** *level*]

*level* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows all configured maintenance domains.

```
Console#show ethernet cfm md
MD Index  MD Name          Level  MIP Creation  Archive Hold Time (m.)
-----  -
          1 rd              0     default      100
Console#
```

**show ethernet cfm ma** This command displays the configured maintenance associations.

### Syntax

**show ethernet cfm ma [level *level*]**

*level* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

For a description of the values displayed in the CC Interval field, refer to the [ethernet cfm cc ma interval](#) command.

### Example

This example shows all configured maintenance associations.

```
Console#show ethernet cfm ma
MD Name      MA Index MA Name      Primary VID  CC Interval MIP Creation
-----
steve        1 voip      1            4 Default
Console#
```

**show ethernet cfm maintenance-points local** This command displays the maintenance points configured on this device.  
**Syntax**

**show ethernet cfm maintenance-points local**  
{**mep** [**domain** *domain-name* | **interface** *interface* | **level** *level-id*] | **mip** [**domain** *domain-name* | **level** *level-id*]}

**mep** – Displays only local maintenance end points.

**mip** – Displays only local maintenance intermediate points.

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*interface* – Displays CFM status for the specified interface.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*level-id* – Maintenance level for this domain. (Range: 0-7)

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Command Usage

- ◆ Use the **mep** keyword with this command to display the MEPs configured on this device as DSAPs through the [ethernet cfm mep](#) command.
- ◆ Using the **mip** keyword with this command to display the MIPs generated on this device by the CFM protocol when the mip-creation method is set to either “default” or “explicit” by the [ethernet cfm domain](#) command or the [ma index name](#) command.

#### Example

This example shows all MEPs configured on this device for maintenance domain rd.

```

Console#show ethernet cfm maintenance-points local mep
MPID MD Name          Level Direct VLAN Port      CC Status MAC Address
-----
  1 rd                 0 UP           1 Eth 1/ 1 Enabled 00-12-CF-3A-A8-C0
Console#

```

**show ethernet cfm maintenance-points local detail mep** This command displays detailed CFM information about a local MEP in the continuity check database.

#### Syntax

**show ethernet cfm maintenance-points local detail mep** [**domain** *domain-name* | **interface** *interface* | **level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*interface* – Displays CFM status for the specified interface.

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

*level-id* – Maintenance level for this domain. (Range: 0-7)

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Example

This example shows detailed information about the local MEP on port 1.

```
Console#show ethernet cfm maintenance-points local detail mep interface
ethernet 1/1
MEP Settings:
-----
MPID                : 1
MD Name             : vopu
MA Name             : r&d
MA Name Format       : Character String
Level               : 0
Direction           : Up
Interface           : Eth 1/ 1
CC Status           : Enabled
MAC Address         : 00-E0-0C-00-00-FD
Defect Condition    : No Defect
Received RDI        : False
AIS Status          : Enabled
AIS Period          : 1 seconds
AIS Transmit Level  : Default
Suppress Alarm      : Disabled
Suppressing Alarms  : Disabled

Console#
```

**Table 149: show ethernet cfm maintenance-points local detail mep - display**

| Field              | Description  |
|--------------------|--|
| MPID               | MEP identifier   |
| MD Name            | The maintenance domain for this entry.   |
| MA Name            | Maintenance association to which this remote MEP belongs   |
| MA Name Format     | The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID   |
| Level              | Maintenance level of the local maintenance point   |
| Direction          | The direction in which the MEP faces on the Bridge port (up or down).  |
| Interface          | The port to which this MEP is attached.  |
| CC Status          | Shows if the MEP will generate CCM messages.   |
| MAC Address        | MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been received or the local MEP record times out, the address will be set to the initial value of all Fs.) |
| Defect Condition   | Shows the defect detected on the MEP.  |
| Received RDI       | Receive status of remote defect indication (RDI) messages on the MEP.  |
| AIS Status         | Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.  |
| AIS Period         | The interval at which AIS information is sent.   |
| AIS Transmit Level | The maintenance level at which AIS information will be sent for the specified MEP.   |
| Suppress Alarm     | Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.   |
| Suppressing Alarms | Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.  |

**show ethernet cfm  
maintenance-points  
remote detail**

This command displays detailed CFM information about a remote MEP in the continuity check database.

**Syntax**

**show ethernet cfm maintenance-points remote detail**

{**mac** *mac-address* | **mpid** *mpid*}  
[**domain** *domain-name* | **level** *level-id* | **ma** *ma-name*]

*mac-address* – MAC address of a remote maintenance point.  
This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*mpid* – Maintenance end point identifier. (Range: 1-8191)

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Authorized maintenance level for this domain. (Range: 0-7)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Use the **mpid** keyword with this command to display information about a specific maintenance point, or use the **mac** keyword to display information about all maintenance points that have the specified MAC address.

### Example

This example shows detailed information about the remote MEP designated by MPID 2.

```
Console#show ethernet cfm maintenance-points remote detail mpid 2
MAC Address           : 00-0D-54-FC-A2-73
Domain/Level          : voip / 3
MA Name               : rd
Primary VLAN          : 1
MPID                  : 2
Incoming Port         : Eth 1/ 2
CC Lifetime           : 645 seconds
Age of Last CC Message : 2 seconds
Frame Loss            : 137
CC Packet Statistics  : 647/1
Port State            : Up
Interface State       : Up
Crosscheck Status     : Enabled

Console#
```

**Table 150: show ethernet cfm maintenance-points remote detail - display**

| Field                                 | Description  |
|---------------------------------------|--|
| MAC Address                           | MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all Fs.) |
| Domain/Level                          | Maintenance domain and level of the remote maintenance point   |
| MA Name                               | Maintenance association to which this remote MEP belongs   |
| Primary VLAN                          | VLAN to which this MEP belongs   |
| MPID                                  | MEP identifier   |
| Incoming Port                         | Port to which this remote MEP is attached.   |
| CC Lifetime                           | Length of time to hold messages about this MEP in the CCM database   |
| Age of Last CC Message                | Length of time the last CCM message about this MEP has been in the CCM database  |
| Frame Loss                            | Percentage of transmitted frames lost  |
| CC Packet Statistics (received/error) | The number of CCM packets received successfully and those with errors  |

**Table 150: show ethernet cfm maintenance-points remote detail - display**

| Field             | Description  |
|-------------------|--|
| Port State        | Port states include:<br>Up – The port is functioning normally.<br>Blocked – The port has been blocked by the Spanning Tree Protocol.<br>No port state – Either no CCM has been received, or no port status TLV was received in the last CCM.   |
| Interface State   | Interface states include:<br>No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM.<br>Up – The interface is ready to pass packets.<br>Down – The interface cannot pass packets.<br>Testing – The interface is in some test mode.<br>Unknown – The interface status cannot be determined for some reason.<br>Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event.<br>Not Present – Some component of the interface is missing.<br>isLowerLayerDown – The interface is down due to state of the lower layer interfaces. |
| Crosscheck Status | Shows if crosscheck function has been enabled.   |

## Continuity Check Operations

**ethernet cfm cc ma interval** This command sets the transmission delay between continuity check messages (CCMs). Use the **no** form to restore the default settings.

### Syntax

**ethernet cfm cc md** *domain-name* **ma** *ma-name* **interval** *interval-level*

**no ethernet cfm cc ma** *ma-name* **interval**

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*interval-level* – The transmission delay between connectivity check messages. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time.

(CCM interval field options: 4 - 1 second, 5 - 10 seconds, 6 - 1 minute, 7 - 10 minutes)

### Default Setting

4 (1 second)

### Command Mode

Global Configuration

### Command Usage

- ◆ CCMs provide a means to discover other MEPs and to detect connectivity failures in an MA. If any MEP fails to receive three consecutive CCMs from any other MEPs in its MA, a connectivity failure is registered. The interval at which

CCMs are issued should therefore be configured to detect connectivity problems in a timely manner, as dictated by the nature and size of the MA.

- ◆ The maintenance of a MIP CCM database by a MIP presents some difficulty for bridges carrying a large number of Service Instances, and for whose MEPs are issuing CCMs at a high frequency. For this reason, slower CCM transmission rates may have to be used.

### Example

This example sets the transmission delay for continuity check messages to level 7 (60 seconds).

```
Console(config)#ethernet cfm cc md voip ma rd interval 7
Console(config)#
```

### Related Commands

[ethernet cfm cc enable \(756\)](#)

**ethernet cfm cc enable** This command enables the transmission of continuity check messages (CCMs) within a specified maintenance association. Use the **no** form to disable the transmission of these messages.

### Syntax

**[no] ethernet cfm cc enable md** *domain-name* **ma** *ma-name*

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- ◆ CCMs are multicast periodically by a MEP in order to discover other MEPs in the same MA, and to assure connectivity to all other MEPs/MIPs in the MA.
- ◆ Each CCM received is checked to verify that the MEP identifier field sent in the message does not match its own MEPID, which would indicate a duplicate MEP or network loop. If these error types are not found, the CCM is stored in the MEP's local database until aged out.
- ◆ If a maintenance point fails to receive three consecutive CCMs from any other MEP in the same MA, a connectivity failure is registered.

- ◆ If a maintenance point receives a CCM with an invalid MEPID or MA level or an MA level lower than its own, a failure is registered which indicates a configuration error or cross-connect error (i.e., overlapping MAs).

### Example

This example enables continuity check messages for the specified maintenance association.

```
Console(config)#ethernet cfm cc enable md voip ma rd  
Console(config)#
```

**snmp-server enable traps ethernet cfm cc** This command enables SNMP traps for CFM continuity check events. Use the **no** form to disable these traps.

### Syntax

**[no] snmp-server enable traps ethernet cfm cc [config | loop | mep-down | mep-up]**

**config** – Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.

**loop** – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.

**mep-down** – Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.

**mep-up** – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which has an expired entry in the archived database.

### Default Setting

All continuity checks are enabled.

### Command Mode

Global Configuration

### Command Usage

All mep-up traps are suppressed when cross-checking of MEPs is enabled because cross-check traps include more detailed status information.

### Example

This example enables SNMP traps for mep-up events.

```
Console(config)#snmp-server enable traps ethernet cfm cc mep-up
Console(config)#
```

### Related Commands

[ethernet cfm mep crosscheck \(763\)](#)

### mep archive-hold-time

This command sets the time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. Use the **no** form to restore the default setting.

### Syntax

**mep archive-hold-time** *hold-time*

*hold-time* – The time to retain data for a missing MEP.  
(Range: 1-65535 minutes)

### Default Setting

100 minutes

### Command Mode

CFM Domain Configuration

### Command Usage

A change to the hold time only applies to entries stored in the database after this command is entered.

### Example

This example sets the aging time for missing MEPs in the CCM database to 30 minutes.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep archive-hold-time 30
Console(config-ether-cfm)#
```

### clear ethernet cfm maintenance-points remote

This command clears the contents of the continuity check database.

### Syntax

**clear ethernet cfm maintenance-points remote** [**domain** *domain-name* |  
**level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Use this command without any keywords to clear all entries in the CCM database. Use the **domain** keyword to clear the CCM database for a specific domain, or the **level** keyword to clear it for a specific maintenance level.

### Example

```
Console#clear ethernet cfm maintenance-points remote domain voip  
Console#
```

**clear ethernet cfm errors** This command clears continuity check errors logged for the specified maintenance domain or maintenance level.

### Syntax

**clear ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Maintenance level. (Range: 0-7)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Use this command without any keywords to clear all entries in the error database. Use the **domain** keyword to clear the error database for a specific domain, or the **level** keyword to clear it for a specific maintenance level.

### Example

```
Console#clear ethernet cfm errors domain voip  
Console#
```

**show ethernet cfm errors** This command displays the CFM continuity check errors logged on this device.

**Syntax**

**show ethernet cfm errors** [**domain** *domain-name* | **level** *level-id*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*level-id* – Authorized maintenance level for this domain. (Range: 0-7)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

```

Console#show ethernet cfm errors
Level VLAN MPID Interface Remote MAC Reason MA Name
-----
5 2 40 Eth 1/1 ab.2f.9c.00.05.01 LEAK provider_1_2
Console#
    
```

**Table 151: show ethernet cfm errors - display description**

| Field      | Description  |
|------------|--|
| Level      | Maintenance level associated with this entry.  |
| VLAN       | VLAN in which this error occurred.   |
| MPID       | Identifier of remote MEP.  |
| Interface  | Port at which the error was recorded   |
| Remote MAC | MAC address of remote MEP.   |
| Reason     | Error types include:<br>LEAK – MA x is associated with a specific VID list*, one or more of the VIDs in this MA can pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA y, at a higher maintenance level, and associated with at least one of the VID(s) also in MA x, does have a MEP configured on the bridge port.<br>VIDS – MA x is associated with a specific VID list* on this MA on the bridge port, and some other MA y, associated with at least one of the VID(s) also in MA x, also has an Up MEP configured facing inward (up) on some bridge port.<br>EXCESS_LEV – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.<br>OVERLAP_LEV – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities. |
| MA         | The maintenance association for this entry.  |

\* This definition is based on the IEEE 802.1ag standard. Current software for this switch only supports a single VLAN per MA. However, since it may interact with other devices which support multiple VLAN assignments per MA, this error message may be reported.

## Cross Check Operations

**ethernet cfm mep crosscheck start-delay** This command sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm mep crosscheck start-delay** *delay*

*delay* – The time a device waits for remote MEPs to come up before the cross-check is started. (Range: 1-65535 seconds)

### Default Setting

30 seconds

### Command Mode

Global Configuration

### Command Usage

- ◆ This command sets the delay that a device waits for a remote MEP to come up, and it starts cross-checking the list of statically configured remote MEPs in the local maintenance domain against the MEPs learned through CCMs.
- ◆ The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps.

### Example

This example sets the maximum delay before starting the cross-check process.

```
Console(config)#ethernet cfm mep crosscheck start-delay 60
Console(config)#
```

**snmp-server enable traps ethernet cfm crosscheck** This command enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages (CCMs). Use the **no** form to restore disable these traps.

### Syntax

**[no] snmp-server enable traps ethernet cfm crosscheck** [**ma-up** | **mep-missing** | **mep-unknown**]

**ma-up** – Sends a trap when all remote MEPs in an MA come up.

**mep-missing** – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list.

**mep-unknown** – Sends a trap if an unconfigured MEP comes up.

### Default Setting

All continuity checks are enabled.

### Command Mode

Global Configuration

### Command Usage

- ◆ For this trap type to function, cross-checking must be enabled on the required maintenance associations using the `ethernet cfm mep crosscheck` command.
- ◆ A mep-missing trap is sent if cross-checking is enabled (with the `ethernet cfm mep crosscheck` command), and no CCM is received for a remote MEP configured in the static list (with the `mep crosscheck mpid` command).
- ◆ A mep-unknown trap is sent if cross-checking is enabled, and a CCM is received from a remote MEP that is not configured in the static list.
- ◆ A ma-up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association.

### Example

This example enables SNMP traps for mep-unknown events detected in cross-check operations.

```
Console(config)#snmp-server enable traps ethernet cfm crosscheck mep-unknown  
Console(config)#
```

**mep crosscheck mpid** This command statically defines a remote MEP in a maintenance association. Use the **no** form to remove a remote MEP.

### Syntax

**[no] mep crosscheck mpid mpid ma ma-name**

*mpid* – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

### Default Setting

No remote MEPs are configured.

### Command Mode

CFM Domain Configuration

### Command Usage

- ◆ Use this command to statically configure remote MEPs that exist inside the maintenance association. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.
- ◆ Remote MEPs can only be configured with this command if domain service access points (DSAPs) have already been created with the `ethernet cfm mep` command at the same maintenance level and in the same MA. DSAPs are MEPs that exist on the edge of the domain, and act as primary service access points for end-to-end cross-check, loop-back, and link-trace functions.

### Example

This example defines a static MEP for the specified maintenance association.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1
Console(config-ether-cfm)#mep crosscheck mpid 2 ma rd
Console(config-ether-cfm)#
```

### ethernet cfm mep crosscheck

This command enables cross-checking between the static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through continuity check messages (CCMs). Use the **disable** keyword to stop the cross-check process.

### Syntax

**ethernet cfm mep crosscheck** {**enable** | **disable**} **md** *domain-name* **ma** *ma-name*

**enable** – Starts the cross-check process.

**disable** – Stops the cross-check process.

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – MA name. (Range: 1-43 alphanumeric characters)

### Default Setting

Disabled

### Command Mode

Privileged Exec

### Command Usage

- ◆ Before using this command to start the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the `mep crosscheck mpid` command. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.

- ◆ The cross-check process is disabled by default, and must be manually started using this command with the **enable** keyword.

### Example

This example enables cross-checking within the specified maintenance association.

```
Console#ethernet cfm mep crosscheck enable md voip ma rd
Console#
```

### show ethernet cfm maintenance-points remote crosscheck

This command displays information about remote MEPs statically configured in a cross-check list.

### Syntax

#### show ethernet cfm maintenance-points remote crosscheck

[**domain** *domain-name* | **mpid** *mpid*]

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*mpid* – Maintenance end point identifier. (Range: 1-8191)

### Default Setting

None

### Command Mode

Privileged Exec

### Example

This example shows all remote MEPs statically configured on this device.

```
Console#show ethernet cfm maintenance-points remote crosscheck
MPID  MA Name                Level  VLAN  MEP Up  Remote MAC
-----
  2   downtown                4      2   Yes    00-0D-54-FC-A2-73
Console#
```

## Link Trace Operations

### ethernet cfm linktrace cache

This command enables caching of CFM data learned through link trace messages. Use the **no** form to disable caching.

### Syntax

[**no**] **ethernet cfm linktrace cache**

### Default Setting

Enabled

### Command Mode

Global Configuration

### Command Usage

- ◆ A link trace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the link trace message reaches its destination or can no longer be forwarded.
- ◆ Use this command to enable the link trace cache to store the results of link trace operations initiated on this device. Use the [ethernet cfm linktrace](#) command to transmit a link trace message.
- ◆ Link trace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.

### Example

This example enables link trace caching.

```
Console(config)#ethernet cfm linktrace cache  
Console(config)#
```

**ethernet cfm linktrace cache hold-time** This command sets the hold time for CFM link trace cache entries. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm linktrace cache hold-time** *minutes*

*minutes* – The aging time for entries stored in the link trace cache.  
(Range: 1-65535 minutes)

### Default Setting

100 minutes

### Command Mode

Global Configuration

### Command Usage

Before setting the aging time for cache entries, the cache must first be enabled with the [ethernet cfm linktrace cache](#) command.

### Example

This example sets the aging time for entries in the link trace cache to 60 minutes.

```
Console(config)#ethernet cfm linktrace cache hold-time 60  
Console(config)#
```

**ethernet cfm linktrace cache size** This command sets the maximum size for the link trace cache. Use the **no** form to restore the default setting.

### Syntax

**ethernet cfm linktrace cache size** *entries*

*entries* – The number of link trace responses stored in the link trace cache.  
(Range: 1-4095 entries)

### Default Setting

100 entries

### Command Mode

Global Configuration

### Command Usage

- ◆ Before setting the cache size, the cache must first be enabled with the [ethernet cfm linktrace cache](#) command.
- ◆ If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased with this command, or purged with the [clear ethernet cfm linktrace-cache](#) command.

### Example

This example limits the maximum size of the link trace cache to 500 entries.

```
Console(config)#ethernet cfm linktrace cache size 500  
Console(config)#
```

**ethernet cfm linktrace** This command sends CFM link trace messages to the MAC address of a remote MEP.

### Syntax

```
ethernet cfm linktrace {dest-mep destination-mpid | src-mep source-mpid  
{dest-mep destination-mpid | mac-address} | mac-address} md domain-name  
ma ma-name [tll number]
```

*destination-mpid* – The identifier of a remote MEP that is the target of the link trace message. (Range: 1-8191)

*source-mpid* – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)

*mac-address* – MAC address of a remote MEP that is the target of the link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*number* – The time to live of the linktrace message. (Range: 1-255 hops)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

- ◆ Link trace messages can be targeted to MEPs, not MIPs. Before sending a link trace message, be sure you have configured the target MEP for the specified MA.
- ◆ If the MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the [show ethernet cfm maintenance-points remote crosscheck](#) command to verify that a MAC address has been learned for the target MEP.
- ◆ Link trace messages (LTMs) are sent as multicast CFM frames, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the LTM reaches its destination or can no longer be forwarded.
- ◆ Link trace messages are used to isolate faults. However, this task can be difficult in an Ethernet environment, since each node is connected through multipoint links. Fault isolation is even more challenging since the MAC address of the target node can age out in several minutes. This can cause the traced path to vary over time, or connectivity lost if faults cause the target MEP to be isolated from other MEPs in an MA.

- ◆ When using the command line or web interface, the source MEP used by to send a link trace message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

### Example

This example sends a link trace message to the specified MEP with a maximum hop count of 25.

```
Console#linktrace ethernet dest-mep 2 md voip ma rd ttl 25
Console#
```

**clear ethernet cfm linktrace-cache** This command clears link trace messages logged on this device.

**Command Mode**  
Privileged Exec

### Example

```
Console#clear ethernet cfm linktrace-cache
Console#
```

**show ethernet cfm linktrace-cache** This command displays the contents of the link trace cache.

**Command Mode**  
Privileged Exec

### Example

```
Console#show ethernet cfm linktrace-cache
Hops MA          IP / Alias      Ingress MAC      Ing. Action Relay
Egress MAC      Egr. Action
-----
  2 rd          192.168.0.6    00-12-CF-12-12-2D ingOk      Hit
                Not Forwarded
Console#
```

**Table 152: show ethernet cfm linktrace-cache - display description**

| Field       | Description   |
|-------------|---|
| Hops        | The number hops taken to reach the target MEP.  |
| MA          | Name of the MA to which this device belongs.  |
| IP/Alias    | IP address or alias of the target device's CPU.   |
| Forwarded   | Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP. |
| Ingress MAC | MAC address of the ingress port on the target device.   |

**Table 152: show ethernet cfm linktrace-cache - display description** (Continued)  
(Continued)

| Field       | Description  |
|-------------|--|
| Egress MAC  | MAC address of the egress port on the target device.   |
| Ing. Action | Action taken on the ingress port:<br>IngOk – The target data frame passed through to the MAC Relay Entity.<br>IngDown – The bridge port’s MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port’s MAC_Operational parameter to be false.<br>IngBlocked – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state.<br>IngVid – The ingress port is not in the member set of the LTM’s VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering. |
| Egr. Action | Action taken on the egress port:<br>EgrOk – The targeted data frame was forwarded.<br>EgrDown – The Egress Port can be identified, but that bridge port’s MAC_Operational parameter is false.<br>EgrBlocked – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in the forwarding state.<br>EgrVid – The Egress Port can be identified, but the bridge port is not in the LTM’s VID member set, and was therefore filtered by egress filtering.   |
| Relay       | Relay action:<br>FDB – Target address found in forwarding database.<br>MPDB – Target address found in the maintenance point database.<br>HIT – Target located on this device.  |

## Loopback Operations

**ethernet cfm loopback** This command sends CFM loopback messages to a MAC address for a MEP or MIP.

### Syntax

```
ethernet cfm loopback {dest-mep destination-mpid | src-mep source-mpid  
{dest-mep destination-mpid | mac-address} | mac-address} md domain-name  
ma ma-name [count transmit-count] [pattern padding-value]  
[priority priority-value] [size packet-size]
```

*destination-mpid* – The identifier of a MEP that is the target of the loopback message. (Range: 1-8191)

*source-mpid* – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)

*mac-address* – MAC address of the remote maintenance point that is the target of the loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*transmit-count* – The number of times the loopback message is sent. (Range: 1-1024)

*padding-value* – Padding characters used to fill the data TLV in a loopback message. (Range: Any hexadecimal characters; Default: 0x0)

*priority-value* – Priority assigned to the loopback message (Range:0-7; Default: 7)

*packet-size* – The size of the loopback message. (Range: 64-1518 bytes)

### Default Setting

Loop back count: One loopback message is sent.

Loop back size: 64 bytes

### Command Mode

Privileged Exec

### Command Usage

- ◆ Use this command to test the connectivity between maintenance points. If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.
- ◆ The point from which the loopback message is transmitted (i.e., the DSAP) and the target maintenance point specified in this command must be within the same MA.
- ◆ Loop back messages can be used for fault verification and isolation after automatic detection of a fault or receipt of some other error report. Loopback

messages can also be used to confirm the successful restoration or initiation of connectivity. The receiving maintenance point should respond to the loop back message with a loopback reply.

- ◆ When using the command line or web interface, the source MEP used by to send a loopback message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

### Example

This example sends a loopback message to the specified remote MEP.

```
Console#ethernet cfm loopback dest-mep 1 md voip ma rd  
Console#
```

## Fault Generator Operations

**mep fault-notify alarm-time** This command sets the time a defect must exist before a fault alarm is issued. Use the **no** form to restore the default setting.

### Syntax

**mep fault-notify alarm-time** *alarm-time*

**no fault-notify alarm-time**

*alarm-time* – The time that one or more defects must be present before a fault alarm is generated. (Range: 3-10 seconds)

### Default Setting

3 seconds

### Command Mode

CFM Domain Configuration

### Command Usage

A fault alarm is issued when the MEP fault notification generator state machine detects that a time period configured by this command has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by the [mep fault-notify lowest-priority](#) command.

### Example

This example set the delay time before generating a fault alarm.

```
Console(config)#ethernet cfm domain index 1 name voip level 3  
Console(config-ether-cfm)#mep fault-notify alarm-time 10  
Console(config-ether-cfm)#
```

**mep fault-notify lowest-priority** This command sets the lowest priority defect that is allowed to generate a fault alarm. Use the **no** form to restore the default setting.

### Syntax

**mep fault-notify lowest-priority** *priority*

**no fault-notify lowest-priority**

*priority* – Lowest priority default allowed to generate a fault alarm.  
(Range: 1-6)

### Default Setting

Priority level 2

### Command Mode

CFM Domain Configuration

### Command Usage

- ◆ A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that a configured time period (see the [mep fault-notify alarm-time](#) command) has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by this command. The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (see the [mep fault-notify reset-time](#) command) without a defect indication. The normal procedure upon receiving a fault alarm is to inspect the reporting MEP's managed objects using an appropriate SNMP software tool, diagnose the fault, correct it, re-examine the MEP's managed objects to see whether the MEP fault notification generator state machine has been reset, and repeat those steps until the fault is resolved.
- ◆ Only the highest priority defect currently detected is reported in the fault alarm.
- ◆ Priority defects include the following items:

**Table 153: Remote MEP Priority Levels**

| Priority Level | Level Name    | Description   |
|----------------|---------------|---|
| 1              | allDef        | All defects.  |
| 2              | macRemErrXcon | DefMACstatus, DefRemoteCCM, DefErrorCCM, or DefXconCCM. |
| 3              | remErrXcon    | DefErrorCCM, DefXconCCM or DefRemoteCCM.                |
| 4              | errXcon       | DefErrorCCM or DefXconCCM.                              |
| 5              | xcon          | DefXconCCM  |
| 6              | noXcon        | No defects DefXconCCM or lower are to be reported.      |

**Table 154: MEP Defect Descriptions**

| Field        | Description  |
|--------------|--|
| DefMACstatus | Either some remote MEP is reporting its Interface Status TLV as not isUp, or all remote MEPs are reporting a Port Status TLV that contains some value other than psUp. |
| DefRemoteCCM | The MEP is not receiving valid CCMs from at least one of the remote MEPs.  |
| DefErrorCCM  | The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.  |
| DefXconCCM   | The MEP has received at least one CCM from either another MAID or a lower MD Level whose CCM Interval has not yet timed out.   |

### Example

This example sets the lowest priority defect that will generate a fault alarm.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify lowest-priority 1
Console(config-ether-cfm)#
```

### mep fault-notify reset-time

This command configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. Use the **no** form to restore the default setting.

### Syntax

**mep fault-notify reset-time** *reset-time*

**no fault-notify reset-time**

*reset-time* – The time that must pass without any further defects indicated before another fault alarm can be generated. (Range: 3-10 seconds)

### Default Setting

10 seconds

### Command Mode

CFM Domain Configuration

### Example

This example sets the reset time after which another fault alarm can be generated.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify reset-time 7
Console(config-ether-cfm)#
```

**show ethernet cfm fault-notify-generator** This command displays configuration settings for the fault notification generator.

**Syntax**

**show ethernet cfm fault-notify-generator mep *mpid***

*mpid* – Maintenance end point identifier. (Range: 1-8191)

**Default Setting**

None

**Command Mode**

Privileged Exec

**Example**

This example shows the fault notification settings configured for one MEP.

```
Console#show ethernet cfm fault-notify-generator mep 1
MD Name      MA Name      Highest Defect Lowest Alarm  Alarm Time Reset Time
-----
          voip          rd none          macRemErrXcon  3sec.    10sec.
Console#
```

**Table 155: show fault-notify-generator - display description**

| Field         | Description   |
|---------------|---|
| MD Name       | The maintenance domain for this entry.  |
| MA Name       | The maintenance association for this entry.   |
| Hihest Defect | The highest defect that will generate a fault alarm. (This is disabled by default.)   |
| Lowest Alarm  | The lowest defect that will generate a fault alarm (see the <a href="#">mep fault-notify lowest-priority</a> command).  |
| Alarm Time    | The time a defect must exist before a fault alarm is issued (see the <a href="#">mep fault-notify alarm-time</a> , command).  |
| Reset Time    | The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued (see the <a href="#">mep fault-notify reset-time</a> command). |

## Delay Measure Operations

**ethernet cfm delay-measure two-way** This command sends periodic delay-measure requests to a specified MEP within a maintenance association.

### Syntax

**ethernet cfm delay-measure two-way** [**src-mep** *source-mpid*] {**dest-mep** *destination-mpid* | *mac-address*} **md** *domain-name* **ma** *ma-name* [**count** *transmit-count*] [**interval** *interval*] [**size** *packet-size*] [**timeout** *timeout*]

*source-mpid* – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)

*destination-mpid* – The identifier of a remote MEP that is the target of the delay-measure message. (Range: 1-8191)

*mac-address* – MAC address of a remote MEP that is the target of the delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

*domain-name* – Domain name. (Range: 1-43 alphanumeric characters)

*ma-name* – Maintenance association name. (Range: 1-43 alphanumeric characters)

*count* – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5)

*interval* – The transmission delay between delay-measure messages. (Range: 1-5 seconds)

*packet-size* – The size of the delay-measure message. (Range: 64-1518 bytes)

*timeout* – The timeout to wait for a response. (Range: 1-5 seconds)

### Default Setting

Count: 5

Interval: 1 second

Size: 64 bytes

Timeout: 5 seconds

### Command Mode

Privileged Exec

### Command Usage

- ◆ Delay measurement can be used to measure frame delay and frame delay variation between MEPs.
- ◆ A local MEP must be configured for the same MA before you can use this command.

- ◆ If a MEP is enabled to generate frames with delay measurement (DM) information, it periodically sends DM frames to its peer MEP in the same MA., and expects to receive DM frames back from it.
- ◆ Frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with DM request information with the TxTimeStampf (Timestamp at the time of sending a frame with DM request information), and the receiving MEP responds with a frame with DM reply information with TxTimeStampf copied from the DM request information, RxTimeStampf (Timestamp at the time of receiving a frame with DM request information), and TxTimeStamptb (Timestamp at the time of transmitting a frame with DM reply information):

$$\text{Frame Delay} = (\text{RxTimeStampb} - \text{TxTimeStampf}) - (\text{TxTimeStamptb} - \text{RxTimeStampf})$$

- ◆ The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

### Example

This example sends periodic delay-measure requests to a remote MEP.

```
Console#ethernet cfm delay-measure two-way dest-mep 1 md voip ma rd
Type ESC to abort.
Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.
Sequence  Delay Time (ms.)  Delay Variation (ms.)
-----  -
          1                < 10                0
          2                < 10                0
          3                < 10                0
          4                 40                40
          5                < 10                40
Success rate is 100% (5/5), delay time min/avg/max=0/8/40 ms.
Average frame delay variation is 16 ms.
Console#
```

## OAM Commands

The switch provides OAM (Operation, Administration, and Maintenance) 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, loop back testing, and displaying device information.

**Table 156: OAM Commands**

| Command   | Function   | Mode  |
|---|--|-------|
| <code>efm oam</code>                                | Enables OAM services   | IC    |
| <code>efm oam critical-link-event</code>            | Enables reporting of critical event or dying gasp                    | IC    |
| <code>efm oam link-monitor frame</code>             | Enables reporting of errored frame link events                       | IC    |
| <code>efm oam link-monitor frame threshold</code>   | Sets the threshold for errored frame link events                     | IC    |
| <code>efm oam link-monitor frame window</code>      | Sets the monitor period for errored frame link events                | IC    |
| <code>efm oam mode</code>                           | Sets the OAM operational mode to active or passive                   | IC    |
| <code>clear efm oam counters</code>                 | Clears statistical counters for various OAMPDU message types         | PE    |
| <code>clear efm oam event-log</code>                | Clears all entries from the OAM event log for the specified port     | PE    |
| <code>efm oam remote-loopback</code>                | Initiates or terminates remote loopback test                         | PE    |
| <code>efm oam remote-loopback test</code>           | Performs remote loopback test, sending a specified number of packets | PE    |
| <code>show efm oam counters interface</code>        | Displays counters for various OAM PDU message types                  | NE,PE |
| <code>show efm oam event-log interface</code>       | Displays OAM event log   | NE,PE |
| <code>show efm oam remote-loopback interface</code> | Displays results of OAM remote loopback test                         | NE,PE |
| <code>show efm oam status interface</code>          | Displays OAM configuration settings and event counters               | NE,PE |
| <code>show efm oam status remote interface</code>   | Displays information about attached OAM-enabled devices              | NE,PE |

**efm oam** This command enables OAM functions on the specified port. Use the **no** form to disable this function.

### Syntax

**[no] efm oam**

### Default Setting

Disabled

### Command Mode

Interface Configuration

### Command Usage

- ◆ If the remote device also supports OAM, both exchange Information OAMPDUs to establish an OAM link.
- ◆ Not all CPEs support OAM functions, and OAM is therefore disabled by default. If the CPE attached to a port supports OAM, then this functionality must first be enabled by the **efm oam** command to gain access to other remote configuration functions.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam
Console(config-if)#
```

**efm oam critical-link-event** This command enables reporting of critical event or dying gasp. Use the **no** form to disable this function.

### Syntax

**[no] efm oam critical-link-event {critical-event | dying-gasp}**

**critical-event** - If a critical event occurs, the local OAM entity (this switch) indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log.

**dying-gasp** - If an unrecoverable condition occurs, the local OAM entity indicates this by immediately sending a trap message.

### Default Setting

Enabled

### Command Mode

Interface Configuration

### Command Usage

- ◆ Critical events are vendor-specific and may include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.
- ◆ Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.



**Note:** When system power fails, the switch will always send a dying gasp trap message prior to power down.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam critical-link-event dying-gasp
Console(config-if)#
```

**efm oam link-monitor frame** This command enables reporting of errored frame link events. Use the **no** form to disable this function.

### Syntax

**[no] efm oam link-monitor frame**

### Default Setting

Enabled

### Command Mode

Interface Configuration

### Command Usage

- ◆ An errored frame is a frame in which one or more bits are errored.
- ◆ If this feature is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame
Console(config-if)#
```

**efm oam link-monitor frame threshold** This command sets the threshold for errored frame link events. Use the **no** form to restore the default setting.

#### Syntax

**efm oam link-monitor frame threshold** *count*

**no efm oam link-monitor frame threshold**

*count* - The threshold for errored frame link events. (Range: 1-65535)

#### Default Setting

1

#### Command Mode

Interface Configuration

#### Command Usage

If this feature is enabled, an event notification message is sent if the threshold is reached or exceeded within the period specified by the [efm oam link-monitor frame window](#) command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

#### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame threshold 5
Console(config-if)#
```

**efm oam link-monitor frame window** This command sets the monitor period for errored frame link events. Use the **no** form to restore the default setting.

#### Syntax

**efm oam link-monitor frame window** *size*

**no efm oam link-monitor frame window**

*size* - The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 units of 10 milliseconds)

#### Default Setting

10 (units of 100 milliseconds) = 1 second

#### Command Mode

Interface Configuration

#### Command Usage

If this feature is enabled, an event notification message is sent if the threshold specified by the [efm oam link-monitor frame threshold](#) command is reached or

exceeded within the period specified by this command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

### Example

This example set the window size to 5 seconds.

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame window 50
Console(config-if)#
```

**efm oam mode** This command sets the OAM mode on the specified port. Use the **no** form to restore the default setting.

### Syntax

**efm oam mode** {**active** | **passive**}

**no efm oam mode**

**active** - All OAM functions are enabled.

**passive** - All OAM functions are enabled, except for OAM discovery, and sending loopback control OAMPDUs.

### Default Setting

Active

### Command Mode

Interface Configuration

### Command Usage

When set to active mode, the selected interface will initiate the OAM discovery process. When in passive mode, it can only respond to discovery messages.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam mode active
Console(config-if)#
```

**clear efm oam counters** This command clears statistical counters for various OAMPDU message types.

#### Syntax

**clear efm oam counters** [*interface-list*]

*interface-list* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

#### Command Mode

Privileged Exec

#### Example

```
Console#clear efm oam counters
Console#
```

#### Related Commands

[show efm oam counters interface \(785\)](#)

**clear efm oam event-log** This command clears all entries from the OAM event log for the specified port.

#### Syntax

**clear efm oam event-log** [*interface-list*]

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

#### Command Mode

Privileged Exec

#### Example

```
Console#clear efm oam event-log
Console#
```

**efm oam remote-loopback** This command starts or stops OAM loopback test mode to the attached CPE.

#### Syntax

**efm oam remote-loopback** {**start** | **stop**} *interface*

**start** - Starts remote loopback test mode.

**stop** - Stops remote loopback test mode.

*interface* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Command Usage

- ◆ OAM remote loop back can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loop back testing.
- ◆ Use the **efm oam remote-loopback start** command to start OAM remote loop back test mode on the specified port. Afterwards, use the **efm oam remote-loopback test** command to start sending test packets. Then use the **efm oam remote loopback stop** command to terminate testing (if test packets are still being sent) and to terminate loop back test mode.
- ◆ The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode.
- ◆ During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.
- ◆ During loopback testing, both the switch and remote device are permitted to send OAMPDUs to the peer device and to process any OAMPDUs received from the peer.

#### Example

```
Console#efm oam remote-loopback start 1/1
Loopback operation is processing, please wait.
Enter loopback mode succeeded.
Console#
```

**efm oam remote-loopback test** \$\$\$ This command performs a remote loopback test, sending a specified number of packets.

### Syntax

**efm oam remote-loopback test** *interface* [*number-of-packets* [*packet-size*]]

*interface* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

*number-of-packets* - Number of packets to send. (Range: 1-99999999)

*packet-size* - Size of packets to send. (Range: 64-1518 bytes)

### Default Setting

Number of packets: 10,000

Packet size: 64 bytes

### Command Mode

Privileged Exec

### Command Usage

- ◆ You can use this command to perform an OAM remote loopback test on the specified port. The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode.
- ◆ During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.
- ◆ OAM remote loopback can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loopback testing.
- ◆ A summary of the test is displayed after it is finished.

### Example

```

Console#efm oam remote-loopback test 1/1
Loopback test is processing, press ESC to suspend.
....
Port OAM loopback Tx OAM loopback Rx Loss Rate
-----
1/2          1990          1016   48.94 %
Console#

```

**show efm oam counters interface** This command displays counters for various OAM PDU message types.

#### Syntax

**show efm oam counters interface** [*interface-list*]

*interface-list* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

#### Command Mode

Normal Exec, Privileged Exec

#### Example

```

Console#show efm oam counters interface 1/1
Port OAMPDU Type          TX          RX
-----
1/1  Information            1121        1444
1/1  Event Notification      0           0
1/1  Loopback Control        1           0
1/1  Organization Specific  76          0
Console#

```

**show efm oam event-log interface** This command displays the OAM event log for the specified port(s) or for all ports that have logs.

**show efm oam event-log interface** [*interface-list*]

*interface-list* - *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

#### Command Mode

Normal Exec, Privileged Exec

#### Command Usage

- ◆ When a link event occurs, no matter whether the location is local or remote, this information is entered in the OAM event log.
- ◆ When the log system becomes full, older events are automatically deleted to make room for new entries.

**Example**

```

Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 00:24:07 2001/01/01
  "Unit 1, Port 1: Dying Gasp at Remote"
Console#

```

This command can show OAM link status changes for link partner as shown in this example.

```

Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 10:22:55 2013/09/13
  "Unit 1, Port 1: Connection to remote device is up at Local"
 10:22:44 2013/09/13
  "Unit 1, Port 1: Connection to remote device is down at Local"
  <--- When the link is down, this event will be written to OAM event-log
 10:20:02 2013/09/13
  "Unit 1, Port 1: Connection to remote device is up at Local"
  <--- When the link is up, this event will be written to OAM event-log,
Console#clear efm oam event-log
  <--- Use the "clear efm oam event-log" command to clear the event-log.
Console#show efm oam event-log interface 1/1
Console#

```

This command can show OAM dying gasp changes for link partner as shown in this example.

```

Console#show efm oam event-log interface 1/1
  <--- When dying gasp happens and the switch get these packets, it will log
  this event in OAM event-log.
OAM event log of Eth 1/1:
 10:27:21 2013/09/13
  "Unit 1, Port 1: Connection to remote device is down at Local"
 10:27:20 2013/09/13
  "Unit 1, Port 1: Dying Gasp occurred at Remote"
Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 10:28:31 2013/09/13
  "Unit 1, Port 1: Connection to remote device is up at Local"
 10:28:28 2013/09/13
  "Unit 1, Port 1: Dying Gasp clear occurred at Remote"
  <--- When the remote device comes up, the switch will get OAM packets
  without the dying gasp bit and display "dying gasp event clear".
Console#

```

**show efm oam remote-loopback interface** This command displays the results of an OAM remote loopback test.  
Syntax

**show efm oam remote-loopback interface** [*interface-list*]

*interface-list* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

### Command Mode

Normal Exec, Privileged Exec

### Example

```
Console#show efm oam remote-loopback interface 1/1
Port OAM loopback Tx OAM loopback Rx Loss Rate
-----
1/1          10000          9999    0.01 %
Console#
```

**show efm oam status interface** This command displays OAM configuration settings and event counters.

### Syntax

**show efm oam status interface** [*interface-list*] [**brief**]

*interface* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

**brief** - Displays a brief list of OAM configuration states.

### Command Mode

Normal Exec, Privileged Exec

### Example

```
Console#show efm oam status interface 1/1
OAM information of Eth 1/1:
Basic Information:
Admin State           : Enabled
Operation State      : Operational
Mode                  : Active
Remote Loopback       : Disabled
Remote Loopback Status : No loopback
Dying Gasp            : Enabled
Critical Event        : Enabled
```

```

Link Monitor (Errored Frame) : Enabled
Link Monitor:
  Errored Frame Window (100msec) : 10
  Errored Frame Threshold : 1
Console#show efm oam status interface 1/1 brief
$ = local OAM in loopback
* = remote OAM in loopback

Port Admin   Mode   Remote   Dying   Critical Errored
  State      Loopback Gasp    Event   Frame
-----
1/1 Enabled Active Disabled Enabled Enabled Enabled
Console#

```

**show efm oam status remote interface** This command displays information about attached OAM-enabled devices.

### Syntax

**show efm oam status remote interface** [*interface-list*]

*interface-list* - unit/port

*unit* - Unit identifier. (Range: 1)

*port* - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

### Command Mode

Normal Exec, Privileged Exec

### Example

```

Console#show efm oam status remote interface 1/1
Port MAC Address      OUI   Remote   Unidirectional Link   MIB Variable
  Loopback            Retrieval
-----
1/1 00-12-CF-6A-07-F6 000084 Enabled Disabled Enabled Disabled
Console#

```

# 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 157: Address Table Commands**

| Command                       | Function  | Mode |
|-------------------------------|---|------|
| <code>ip domain-list</code>   | Defines a list of default domain names for incomplete host names                              | GC   |
| <code>ip domain-lookup</code> | Enables DNS-based host name-to-address translation  | GC   |
| <code>ip domain-name</code>   | Defines a default domain name for incomplete host names                                       | GC   |
| <code>ip host</code>          | Creates a static IPv4 host name-to-address mapping  | GC   |
| <code>ip name-server</code>   | Specifies the address of one or more name servers to use for host name-to-address translation | GC   |
| <code>ipv6 host</code>        | Creates a static IPv6 host name-to-address mapping  | GC   |
| <code>clear dns cache</code>  | Clears all entries from the DNS cache   | PE   |
| <code>clear host</code>       | Deletes entries from the host name-to-address table   | PE   |
| <code>show dns</code>         | Displays the configuration for DNS services   | PE   |
| <code>show dns cache</code>   | Displays entries in the DNS cache   | PE   |
| <code>show hosts</code>       | Displays the static host name-to-address mapping table  | PE   |

**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 one or more name servers are configured, but DNS is not yet enabled and the switch receives a DHCP packet containing a DNS field with a list of DNS servers, then the switch will automatically enable DNS host name-to-address translation.
- ◆ 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(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:
Console#

```

**Related Commands**[ip domain-name \(791\)](#)

**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 \(791\)](#)

[ip name-server \(793\)](#)

**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 \(789\)](#)  
[ip name-server \(793\)](#)  
[ip domain-lookup \(790\)](#)

**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: 1-127 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
-----
    0   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 \(791\)](#)

[ip domain-lookup \(790\)](#)

**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
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 158: show dns cache - display description**

| Field      | Description   |
|------------|---|
| No.        | The entry number for each resource record.  |
| Flag       | The flag is always "4" indicating a cache entry and therefore unreliable.   |
| Type       | 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. |
| IP Address | The IP address associated with this record.   |
| TTL        | The time to live reported by the name server.   |
| Host       | The host name associated with this record.  |

**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 159: show hosts - display description**

| <b>Field</b> | <b>Description</b>   |
|--------------|--|
| No.          | The entry number for each resource record.   |
| Flag         | The field displays "2" for a static entry, or "4" for a dynamic entry stored in the cache.   |
| Type         | 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. |
| IP Address   | The IP address associated with this record.  |
| TTL          | The time to live reported by the name server. This field is always blank for static entries.   |
| Host         | The host name associated with this record.   |



# 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 160: DHCP Commands**

| Command Group        | Function  |
|----------------------|---|
| DHCP Client          | Allows interfaces to dynamically acquire IP address information |
| DHCP Relay Option 82 | Relays DHCP requests from local hosts to a remote DHCP server   |

## DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

**Table 161: DHCP Client Commands**

| Command   | Function  | Mode |
|---|---|------|
| <i>DHCP for IPv4</i>                            |   |      |
| <code>ip dhcp dynamic-provision</code>          | Enables dynamic provision via DHCP                            | GC   |
| <code>ip dhcp client class-id</code>            | Specifies the DHCP client identifier for an interface         | IC   |
| <code>ip dhcp restart client</code>             | Submits a BOOTP or DHCP client request                        | PE   |
| <code>show ip dhcp dynamic-provision</code>     | Shows the status of dynamic provision via DHCP                | PE   |
| <i>DHCP for IPv6</i>                            |   |      |
| <code>ipv6 dhcp client rapid-commit vlan</code> | Specifies the Rapid Commit option for DHCPv6 message exchange | GC   |
| <code>ipv6 dhcp restart client vlan</code>      | Submits a DHCPv6 client request                               | PE   |
| <code>show ipv6 dhcp duid</code>                | Shows the DHCP Unique Identifier for this switch              | PE   |
| <code>show ipv6 dhcp vlan</code>                | Shows DHCPv6 information for specified interface              | PE   |

## DHCP for IPv4

**ip dhcp dynamic-provision** This command enables dynamic provisioning via DHCP. Use the **no** form to disable this feature.

### Syntax

**[no] ip dhcp dynamic-provision**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

DHCPD is the daemon used by Linux to dynamically configure TCP/IP information for client systems. To support DHCP option 66/67, you have to add corresponding statements to the configuration file of DHCPD. Information on how to complete this process are described in [“Downloading a Configuration File Referenced by a DHCP Server” on page 59](#).

The following are some alternative commands which can be added to the DHCPD to complete the dynamic provisioning process.

By default, the parameters for DHCP option 66/67 are not carried by the reply sent from the DHCP server. To ask for a DHCP reply with option 66/67, the client can inform the server that it is interested in option 66/67 by sending a DHCP request that includes a 'parameter request list' option. Besides this, the client can also send a DHCP request that includes a 'vendor class identifier' option to the server so that the DHCP server can identify the device, and determine what information should be given to requesting device.

The following are two additional sample configurations of the dhcpd.conf file for the server version dhcp-3.0.4rc1, you can choose either one of them.

#### 1. Define the conditions in subnet section:

```
shared-network Sample1 {
    subnet 192.168.1.0 netmask 255.255.255.0 {
# option 55
        option dhcp-parameter-request-list 1,66,67;
# option 66
        option tftp-server-name "192.168.1.1";
# option 67
        option bootfile-name "dhcp_config.cfg ";
    }
}
```

**2.** Define the conditions in class section:

```

class "OPT66_67" { # for option 66/67
# option 124
    match if option vendor-class-identifier = "SMC";
# option 55
    option dhcp-parameter-request-list 1,66,67;
# option 66
    option tftp-server-name "192.168.1.1";
# option 67
    option bootfile-name "dhcp_config.cfg";
}

shared-network Sample2 {
subnet 192.168.1.0 netmask 255.255.255.0 {
    }
    pool {
        allow members of "OPT66_67";
        range 192.168.1.10 192.168.1.20;
    }
}
}

```

**Example**

In the following example enables dhcp dynamic provisioning.

```

Console(config)#ip dhcp dynamic provisioning
Console(config)#

```

**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, using the model number as the string.

**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 162: Options 60, 66 and 67 Statements**

| Option | Statement               |   |
|--------|-------------------------|---|
|        | Keyword                 | Parameter                                       |
| 60     | vendor-class-identifier | a string indicating the vendor class identifier |
| 66     | tftp-server-name        | a string indicating the tftp server name        |
| 67     | bootfile-name           | a string indicating the bootfile name           |

- ◆ 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.

**Table 163: Options 55 and 124 Statements**

| Option | Statement                   |   |
|--------|-----------------------------|---|
|        | Keyword                     | Parameter                                       |
| 55     | dhcp-parameter-request-list | a list of parameters, separated by "            |
| 124    | vendor-class-identifier     | a string indicating the vendor class identifier |

- ◆ 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.

### Example

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

### Related Commands

[ip dhcp restart client \(803\)](#)

**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 12-34-12-34-12-34
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.9 Mask: 255.255.255.0
  DHCP Client Vendor Class ID (text): ECS4810-12M
Console#
```

### Related Commands

[ip address \(814\)](#)

**show ip dhcp dynamic-provision** This command shows the status of dynamic provision via DHCP.

### Command Mode

Privileged Exec

### Example

```
Console#show ip dhcp dynamic provisioning
Dynamic Provision via DHCP Status:  Disabled
Console#
```

## DHCP for IPv6

**ipv6 dhcp client rapid-commit vlan** 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, DHCPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.
- ◆ If the rapid commit option has been enabled on the switch with this 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

```
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 \(826\)](#)

**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-list***

*vlan-list* - 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, 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 Option 82

This section describes commands used to configure the switch to relay DHCP requests from local hosts to a remote DHCP server.

**Table 164: DHCP Relay Option 82 Commands**

| Command  | Function   | Mode |
|--|--|------|
| <a href="#">ip dhcp relay server</a>             | Specifies DHCP server or relay server addresses  | GC   |
| <a href="#">ip dhcp relay information option</a> | Enables DHCP Option 82 information relay, and specifies the frame format for the remote-id | GC   |
| <a href="#">ip dhcp relay information policy</a> | Specifies how to handle DHCP client requests which already contain Option 82 information   | GC   |
| <a href="#">show ip dhcp relay</a>               | Displays the configuration settings for DHCP relay service                                 | PE   |

**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

Global Configuration

### Usage Guidelines

- ◆ DHCP relay service applies to DHCP client requests received on any configured VLAN, both the management VLAN and non-management VLANs.
- ◆ This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled (using the [ip dhcp relay information option](#) command), 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.

### Example

```
Console(config)#ip dhcp relay server 192.168.10.19
Console(config)#
```

### ip dhcp relay information option

This command enables DHCP Option 82 information relay, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the **no** form of this command to disable this feature.

### Syntax

#### ip dhcp relay information option

[**encode no-subtype**]  
[**remote-id** {**ip-address** [**encode** {**ascii** | **hex**}] |  
**mac-address** [**encode** {**ascii** | **hex**}] | **string** *string*}]

**no ip dhcp relay 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** - Includes a MAC address field for the relay agent (that is, the MAC address of the switch's CPU).

**ip-address** - Includes the IP address field for the relay 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

## Command Mode

### Global Configuration

#### Usage Guidelines

- ◆ Using this command with or without any keywords will enable DHCP Option 82 information relay. You must also specify the IP address for at least one active DHCP server (with the `ip dhcp relay server` command). Otherwise, the switch's DHCP relay agent will not be able to forward client requests to a DHCP server.
- ◆ DHCP provides a relay agent information option for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients.
- ◆ When 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. Depending on the selected frame format set for the `remote-id` by this command, this information may specify the MAC address, IP address, or an arbitrary string for the requesting device (that is, the relay agent in this context).
- ◆ By default, the relay agent also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the VLAN ID, stack unit, and port. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them onto the entire VLAN.
- ◆ DHCP request packets received by the switch are handled as follows:
  - If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet *without* option 82 information from the management VLAN or a non-management VLAN, it will add option 82 relay information and the relay agent's address to the DHCP request packet, and then unicast it to the DHCP server.
  - If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet *with* option 82 information from the management VLAN or a non-management VLAN, it will process it according to the configured relay information option policy:
    - If the policy is "replace," the DHCP request packet's option 82 content (the RID and CID sub-option) is replaced with information provided by the switch. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.
    - If the policy is "keep," the DHCP request packet's option 82 content will be retained. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.
    - If the policy is "drop," the original DHCP request packet is flooded onto the VLAN which received the packet but is not relayed.

- ◆ DHCP reply packets received by the relay agent are handled as follows:

When the relay agent receives a DHCP reply packet with Option 82 information over the management VLAN, it first ensures that the packet is destined for itself.

- If the RID in the DHCP reply packet is not identical with that configured on the switch, the option 82 information is retained, and the packet is flooded onto the VLAN through which it was received.
  - If the RID in the DHCP reply packet matches that configured on the switch, it then removes the Option 82 information from the packet, and sends it on as follows:
    - If the DHCP packet's broadcast flag is on, the switch uses the circuit-id information contained in the option 82 information fields to identify the VLAN connected to the requesting client and then broadcasts the DHCP reply packet to this VLAN.
    - If the DHCP packet's broadcast flag is off, the switch uses the circuit-id information in option 82 fields to identify the interface connected to the requesting client and unicasts the reply packet to the client.
- ◆ DHCP packets are flooded onto the VLAN which received them if DHCP relay service is enabled on the switch and any of the following situations apply:
    - There is no DHCP relay server set on the switch, when the switch receives a DHCP packet.
    - A DHCP relay server has been set on the switch, when the switch receives a DHCP request packet with a non-zero relay agent address field (that is not the address of this switch).
    - A DHCP relay server has been set on the switch, when the switch receives DHCP reply packet without option 82 information from the management VLAN.
    - The reply packet contains a valid relay agent address field (that is not the address of this switch), or receives a reply packet with a zero relay agent address through the management VLAN.
    - A DHCP relay server has been set on the switch, and the switch receives a reply packet on a non-management VLAN.
  - ◆ Use the `ip dhcp relay information policy` command to specify how to handle DHCP client request packets which already contain Option 82 information.
  - ◆ DHCP Snooping Information Option 82 (see [page 307](#)) and DHCP Relay Information Option 82 cannot both be enabled at the same time.

### Example

This example enables Option 82, and sets the frame format of the remote ID for the option to use the MAC address of the switch's CPU.

```
Console(config)#ip dhcp relay information option remote-id mac-address  
Console(config)#
```

### Related Commands

[ip dhcp relay information policy \(811\)](#)

[ip dhcp relay server \(807\)](#)

[ip dhcp snooping \(305\)](#)

**ip dhcp relay information policy** This command specifies how to handle client requests which already contain DHCP Option 82 information.

### Syntax

**ip dhcp relay information policy {drop | keep | replace}**

**drop** - Floods the original request packet onto the VLAN that received it instead of relaying it.

**keep** - Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.

**replace** - Replaces the Option 82 information circuit-id and remote-id fields in the client's request packet with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server.

### Default Setting

drop

### Command Mode

Global Configuration

### Usage Guidelines

- ◆ Refer to the Usage Guidelines under the [ip dhcp relay information option](#) command for information on when Option 82 information is processed by the switch.
- ◆ When the Option 82 policy is set to "keep" the original information in the request packet, the frame type specified by the [ip dhcp relay information option](#) command is ignored.

### Example

This example sets the Option 82 policy to keep the client information in the request packet received by the relay agent, and forward this packet on to the DHCP server.

```
Console(config)#ip dhcp relay information policy keep
Console(config)#
```

### Related Commands

[ip dhcp relay information option \(808\)](#)

[ip dhcp relay server \(807\)](#)

[ip dhcp snooping \(305\)](#)

**show ip dhcp relay** This command displays the configuration settings for DHCP relay service.

### Command Mode

Privileged Exec

### Example

```
Console#show ip dhcp relay
Status of DHCP relay information:
Insertion of relay information: enabled.
DHCP option policy: drop.
DHCP relay-server address: 192.168.0.4
                           0.0.0.0
                           0.0.0.0
                           0.0.0.0
                           0.0.0.0
DHCP sub-option format: extra subtype included
DHCP remote id sub-option: mac address (hex encoded)
Console#
```

### Related Commands

[ip dhcp relay server \(807\)](#)

# 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 165: IP Interface Commands**

| Command Group  | Function  |
|----------------|---|
| IPv4 Interface | Configures an IPv4 address for the switch   |
| IPv6 Interface | Configures an IPv6 address for the switch   |
| ND Snooping    | 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 |

## 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 166: IPv4 Interface Commands**

| Command Group            | Function  |
|--------------------------|---|
| Basic IPv4 Configuration | Configures the IP address for interfaces and the gateway router |
| ARP Configuration        | Configures static, dynamic and proxy ARP service                |

**Basic IPv4 Configuration** This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

**Table 167: Basic IP Configuration Commands**

| Command                                 | Function  | Mode   |
|---|---|--------|
| <a href="#">ip address</a>              | Sets the IP address for the current interface                                     | IC     |
| <a href="#">ip default-gateway</a>      | Defines the default gateway through which this switch can reach other subnetworks | GC     |
| <a href="#">show ip default-gateway</a> | Displays the default gateway configured for this device                           | PE     |
| <a href="#">show ip interface</a>       | Displays the IP settings for this device  | PE     |
| <a href="#">show ip traffic</a>         | Displays statistics for IP, ICMP, UDP, TCP and ARP protocols                      | PE     |
| <a href="#">traceroute</a>              | Shows the route packets take to the specified host                                | PE     |
| <a href="#">ping</a>                    | Sends ICMP echo request packets to another node on the network                    | NE, PE |

**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

- ◆ An IP address must be assigned to this device to gain management access over the network or to connect the switch to existing IP subnets. A specific IP address can be manually configured, or the switch 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.
- ◆ 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 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(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(config)#interface vlan 2
Console(config-if)#ip address 10.2.2.1/24
Console(config-if)#
```

### Related Commands

[ip dhcp restart client \(803\)](#)  
[ip default-gateway \(816\)](#)  
[ipv6 address \(825\)](#)

**ip default-gateway** This command specifies the default gateway through which this switch can reach other subnetworks. 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

- ◆ A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
- ◆ A gateway must be defined if the management station is located in a different IP segment.

### 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 \(814\)](#)  
[ipv6 default-gateway \(824\)](#)

**show ip default-gateway** This command shows the IPv4 default gateway configured for this device.

### Default Setting

None

### Command Mode

Privileged Exec

### Example

```
Console#show ip default-gateway
IP default gateway 10.1.0.254
Console#
```

### Related Commands

[ip default-gateway \(816\)](#)

[show ipv6 default-gateway \(833\)](#)

**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 70-72-CF-59-8F-40
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.2.13 Mask: 255.255.255.0
  DHCP Client Vendor Class ID (text): ECS4810-12M
  Craft interface is Administrative Up
  IP Address: 192.168.1.2 Mask: 255.255.255.0
Console#
```

### Related Commands

[ip address \(814\)](#)

[show ipv6 interface \(833\)](#)

**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
    4877 total received
        header errors
        unknown protocols
        address errors
        discards
    4763 delivers
        reassembly request datagrams
        reassembly succeeded
        reassembly failed
IP sent
    forwards datagrams
```

```
5927 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:
2 input
no port errors
other errors
output

TCP Statistics:
4698 input
input errors
5867 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 192.168.0.99, 30 hops max, timeout is 3 seconds

Hop  Packet 1  Packet 2  Packet 3  IP Address
-----
  1   <10 ms   <10 ms   <10 ms   192.168.0.99

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 793](#)) and host name-to-address translation enabled ([page 790](#)). If necessary, local devices can also be specified in the DNS static host table ([page 792](#)).

### Example

```
Console#ping 10.1.0.9
Press ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 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
Console#
```

## Related Commands

[interface \(370\)](#)

**ARP Configuration** This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

**Table 168: Address Resolution Protocol Commands**

| Command                         | Function   | Mode   |
|---------------------------------|--|--------|
| <a href="#">arp timeout</a>     | Sets the time a dynamic entry remains in the ARP cache | GC     |
| <a href="#">clear arp-cache</a> | Deletes all dynamic entries from the ARP cache         | PE     |
| <a href="#">show arp</a>        | Displays entries in the ARP cache                      | NE, PE |

**arp timeout** This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default timeout.

### Syntax

**arp timeout** *seconds*

**no arp timeout**

*seconds* - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 seconds is one day)

### Default Setting

1200 seconds (20 minutes)

### Command Mode

Global Configuration

### Command Usage

- ◆ When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.
- ◆ The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the switch may tie up resources by repeating ARP requests for addresses recently flushed from the table.

### Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp timeout 900
Console(config)#
```

**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)?
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 (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)

IP Address      MAC Address      Type      Interface
-----
10.1.0.0        FF-FF-FF-FF-FF-FF other      VLAN1
10.1.0.254      00-00-AB-CD-00-00 other      VLAN1
10.1.0.255      FF-FF-FF-FF-FF-FF other      VLAN1
145.30.20.23    09-50-40-30-20-10 dynamic     VLAN3

Total entry : 5
Console#
```

## IPv6 Interface

This switch supports the following IPv6 interface commands.

**Table 169: IPv6 Configuration Commands**

| Command  | Function  | Mode   |
|--|---|--------|
| <i>Interface Address Configuration and Utilities</i> |   |        |
| <code>ipv6 default-gateway</code>                    | Sets an IPv6 default gateway for traffic with no known next hop   | GC     |
| <code>ipv6 address</code>                            | Configures an IPv6 global unicast address, and enables IPv6 on an interface   | IC     |
| <code>ipv6 address autoconfig</code>                 | Enables automatic configuration of IPv6 addresses on an interface and enables IPv6 on the interface   | IC     |
| <code>ipv6 address eui-64</code>                     | 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 | IC     |
| <code>ipv6 address link-local</code>                 | Configures an IPv6 link-local address for an interface and enables IPv6 on the interface  | IC     |
| <code>ipv6 enable</code>                             | Enables IPv6 on an interface that has not been configured with an explicit IPv6 address   | IC     |
| <code>ipv6 mtu</code>                                | Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface  | IC     |
| <code>show ipv6 default-gateway</code>               | Displays the current IPv6 default gateway   | NE, PE |
| <code>show ipv6 interface</code>                     | Displays the usability and configured settings for IPv6 interfaces  | NE, PE |
| <code>show ipv6 mtu</code>                           | Displays maximum transmission unit (MTU) information for IPv6 interfaces  | NE, PE |
| <code>show ipv6 traffic</code>                       | Displays statistics about IPv6 traffic  | NE, PE |
| <code>clear ipv6 traffic</code>                      | Resets IPv6 traffic counters  | PE     |
| <code>ping6</code>                                   | Sends IPv6 ICMP echo request packets to another node on the network   | PE     |
| <code>traceroute6</code>                             | Shows the route packets take to the specified host  | PE     |
| <i>Neighbor Discovery</i>                            |   |        |
| <code>ipv6 hop-limit</code>                          | Configures the maximum number of hops used in router advertisements that are originated by this router  | GC     |
| <code>ipv6 nd dad attempts</code>                    | Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection                         | IC     |
| <code>ipv6 nd ns-interval</code>                     | Configures the interval between IPv6 neighbor solicitation retransmissions on an interface  | IC     |
| <code>ipv6 nd raguard</code>                         | Blocks incoming Router Advertisement and Router Redirect packets  | IC     |
| <code>ipv6 nd reachable-time</code>                  | Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred               | IC     |

Table 169: IPv6 Configuration Commands (Continued)

| Command                           | Function   | Mode |
|-----------------------------------|--|------|
| <code>clear ipv6 neighbors</code> | Deletes all dynamic entries in the IPv6 neighbor discovery cache | PE   |
| <code>show ipv6 nd rguard</code>  | Displays the configuration setting for RA Guard                  | PE   |
| <code>show ipv6 neighbors</code>  | Displays information in the IPv6 neighbor discovery cache        | PE   |

## 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 default-gateway**

*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 should be defined if the destination has been assigned an IPv6 address that 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 \(833\)](#)

[ip default-gateway \(816\)](#)

**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 [ip 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 enabled.
Link-local address:
  FE80::2E0:CFE:FE00:FD/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: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 eui-64 \(828\)](#)  
[ipv6 address autoconfig \(826\)](#)  
[show ipv6 interface \(833\)](#)  
[ip address \(814\)](#)

**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) when DHCPv6 is restarted.

### Example

This example assigns a dynamic global unicast address of 2001:DB8:2222:7272:2E0:CFF:FE00:FD to the switch.

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7272:2E0:CFF:FE00:FD/64, subnet is 2001:DB8:2222:7272::/
  64[AUTOCONFIG]
    valid lifetime 2591628 preferred lifetime 604428
Joined group address(es):
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1280 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 \(825\)](#)

[show ipv6 interface \(833\)](#)

**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 enabled.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
  FF02::1:FF00:72
  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 autoconfig \(826\)](#)

[show ipv6 interface \(833\)](#)

**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 enabled.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:2E0:CFE:FE00:FD/64, subnet is 2001:DB8::1:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
  FF02::1:FF19:6779
  FF02::1:FF00:72
  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 enable \(831\)](#)  
[show ipv6 interface \(833\)](#)

**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 828](#)). 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::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
  FF02::1:FF00:72
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1280 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 \(829\)](#)

[show ipv6 interface \(833\)](#)

**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 \(835\)](#)  
[jumbo frame \(112\)](#)

**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: 1-4093)

*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

Privileged 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::2E0:CFE:FE00:FD/64
Global unicast address(es):
```

```

    2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1280 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#

```

**Table 170: show ipv6 interface - display description**

| Field                             | Description   |
|-----------------------------------|---|
| VLAN                              | A VLAN is marked "up" if the switch can send and receive packets on this interface, "down" if a line signal is not present, or "administratively down" if the interface has been disabled by the administrator.   |
| IPv6                              | IPv6 is marked "enable" if the switch can send and receive IP traffic on this interface, "disable" if the switch cannot send and receive IP traffic on this interface, or "stalled" if a duplicate link-local address is detected on the interface.   |
| Link-local address                | Shows the link-local address assigned to this interface   |
| Global unicast address(es)        | Shows the global unicast address(es) assigned to this interface   |
| Joined group address(es)          | <p>In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively.</p> <p>FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.</p> <p>A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.</p> |
| ND DAD                            | Indicates whether (neighbor discovery) duplicate address detection is enabled.  |
| number of DAD attempts            | The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.  |
| ND retransmit interval            | The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection.  |
| ND advertised retransmit interval | The retransmit interval is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.   |
| ND reachable time                 | The amount of time a remote IPv6 node is considered reachable after a reachability confirmation event has occurred  |

**Table 170: show ipv6 interface - display description** (Continued)

| Field                         | Description  |
|-------------------------------|--|
| ND advertised reachable time  | The reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. |
| ND advertised router lifetime | The length of time during which the prefix is valid for on-link determination.   |

This example displays a brief summary of IPv6 addresses configured on the switch.

```

Console#show ipv6 interface brief
Interface      VLAN      IPv6      IPv6 Address
-----
VLAN 1         Up        Up        2001:DB8:2222:7273::72/96
VLAN 1         Up        Up        FE80::2E0:CFE:FE00:FD%1/64
Console#

```

**Related Commands**

[show ip interface \(817\)](#)

**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 171: show ipv6 mtu - display description\***

| Field               | Description  |
|---------------------|--|
| MTU                 | Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path. |
| Since               | Time since an ICMP packet-too-big message was received from this destination.  |
| Destination Address | Address which sent an ICMP packet-too-big message.   |

\* 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
                                total received
                                header errors
                                too big errors
                                no routes
                                address errors
                                unknown protocols
                                truncated packets
                                discards
                                delivers
                                reassembly request datagrams
                                reassembly succeeded
                                reassembly failed

IPv6 sent
                                forwards datagrams
15 requests
                                discards
                                no routes
                                generated fragments
                                fragment succeeded
                                fragment failed

ICMPv6 Statistics:
ICMPv6 received
                                input
                                errors
                                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
                                4 output
                                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
                                1 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 172: show ipv6 traffic - display description**

| Field                        | Description  |
|------------------------------|--|
| <i>IPv6 Statistics</i>       |  |
| <i>IPv6 received</i>         |  |
| total received               | The total number of input datagrams received by the interface, including those received in error.  |
| header errors                | 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.  |
| too big errors               | The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.  |
| no routes                    | The number of input datagrams discarded because no route could be found to transmit them to their destination.   |
| address errors               | 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. |
| unknown protocols            | 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.  |
| truncated packets            | The number of input datagrams discarded because datagram frame didn't carry enough data.   |
| discards                     | 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.  |
| delivers                     | 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.   |
| reassembly request datagrams | 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.   |

**Table 172: show ipv6 traffic - display description** (Continued)

| Field                            | Description   |
|----------------------------------|---|
| reassemble succeeded             | 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.   |
| reassemble failed                | 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. |
| <i>IPv6 sent</i>                 |   |
| forwards datagrams               | 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.   |
| requests                         | 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 <code>ipv6IfStatsOutForwDatagrams</code> .  |
| discards                         | 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 <code>ipv6IfStatsOutForwDatagrams</code> if any such packets met this (discretionary) discard criterion.  |
| no routes                        | The number of input datagrams discarded because no route could be found to transmit them to their destination.  |
| generated fragments              | The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.   |
| fragment succeeded               | The number of IPv6 datagrams that have been successfully fragmented at this output interface.   |
| fragment failed                  | The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.   |
| <i>ICMPv6 Statistics</i>         |   |
| <i>ICMPv6 received</i>           |   |
| input                            | The total number of ICMP messages received by the interface which includes all those counted by <code>ipv6IfIcmpInErrors</code> . 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.  |
| errors                           | The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).  |
| destination unreachable messages | The number of ICMP Destination Unreachable messages received by the interface.  |
| packet too big messages          | The number of ICMP Packet Too Big messages received by the interface.   |
| time exceeded messages           | The number of ICMP Time Exceeded messages received by the interface.  |

**Table 172: show ipv6 traffic - display description** (Continued)

| Field                               | Description   |
|-------------------------------------|---|
| parameter problem message           | The number of ICMP Parameter Problem messages received by the interface.  |
| echo request messages               | The number of ICMP Echo (request) messages received by the interface.   |
| echo reply messages                 | The number of ICMP Echo Reply messages received by the interface.   |
| router solicit messages             | The number of ICMP Router Solicit messages received by the interface.   |
| router advertisement messages       | The number of ICMP Router Advertisement messages received by the interface.   |
| neighbor solicit messages           | The number of ICMP Neighbor Solicit messages received by the interface.   |
| neighbor advertisement messages     | The number of ICMP Neighbor Advertisement messages received by the interface.   |
| redirect messages                   | The number of Redirect messages received by the interface.  |
| group membership query messages     | The number of ICMPv6 Group Membership Query messages received by the interface.   |
| group membership response messages  | The number of ICMPv6 Group Membership Response messages received by the interface.  |
| group membership reduction messages | The number of ICMPv6 Group Membership Reduction messages received by the interface.   |
| <i>ICMPv6 sent</i>                  |   |
| output                              | The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors. |
| destination unreachable messages    | The number of ICMP Destination Unreachable messages sent by the interface.  |
| packet too big messages             | The number of ICMP Packet Too Big messages sent by the interface.   |
| time exceeded messages              | The number of ICMP Time Exceeded messages sent by the interface.  |
| parameter problem message           | The number of ICMP Parameter Problem messages sent by the interface.  |
| echo request messages               | The number of ICMP Echo (request) messages sent by the interface.   |
| echo reply messages                 | The number of ICMP Echo Reply messages sent by the interface.   |
| router solicit messages             | The number of ICMP Router Solicitation messages sent by the interface.  |
| router advertisement messages       | The number of ICMP Router Advertisement messages sent by the interface.   |
| neighbor solicit messages           | The number of ICMP Neighbor Solicit messages sent by the interface.   |
| neighbor advertisement messages     | The number of ICMP Router Advertisement messages sent by the interface.   |
| redirect messages                   | The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.                         |
| group membership query messages     | The number of ICMPv6 Group Membership Query messages sent by the interface.   |
| group membership response messages  | The number of ICMPv6 Group Membership Response messages sent.   |

Table 172: show ipv6 traffic - display description (Continued)

| Field                               | Description   |
|-------------------------------------|---|
| group membership reduction messages | The number of ICMPv6 Group Membership Reduction messages sent.  |
| <i>UDP Statistics</i>               |   |
| input                               | The total number of UDP datagrams delivered to UDP users.   |
| no port errors                      | The total number of received UDP datagrams for which there was no application at the destination port.                                      |
| other errors                        | The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| output                              | The total number of UDP datagrams sent from this entity.  |

**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: 480-512 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: 32 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 790](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 792](#)).
- ◆ 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:CFF:FE00:FC%1/64
Press ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,
  timeout is 3 seconds
response time: 20 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 2
response time: 0 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 3
response time: 0 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%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#
```

**traceroute6** 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:CFE:FE9C:CA10%1/64  
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#
```

## Neighbor Discovery

**ipv6 hop-limit** This command configures the maximum number of hops used in router advertisements that are originated by this router. Use the **no** form to restore the default setting.

### Syntax

**ipv6 hop-limit** *hops*

**no ipv6 hop-limit**

*hops* - The maximum number of hops in router advertisements and all IPv6 packets. (Range: 1-255)

### Default Setting

1

### Command Mode

Global Configuration

### Example

The following sets the hop limit for router advertisements to 64:

```
Console(config)#ipv6 hop-limit 64  
Console(config)#
```

### Related Commands

[show ipv6 neighbors \(849\)](#)

**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 enabled.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
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
Console#
```

### Related Commands

[ipv6 nd ns-interval \(845\)](#)

[show ipv6 neighbors \(849\)](#)

**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

- ◆ 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.

### Example

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
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

[show running-config \(106\)](#)

**ipv6 nd rguard** This command blocks incoming Router Advertisement and Router Redirect packets. Use the no form to disable this feature.

### Syntax

**[no] ipv6 nd rguard**

### 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 rguard
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. Use the **no** form to restore the default setting.

### Syntax

**ipv6 nd reachable-time** *milliseconds*

**no ipv6 nd reachable-time**

*milliseconds* - 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

### 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.
- ◆ The time limit configured by this command allows the switch to detect unavailable neighbors.

- ◆ 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)#ipv6 nd reachable-time 1000
Console(config)#
```

**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 rguard** This command displays the configuration setting for RA Guard.

### Syntax

**show ipv6 nd rguard** [*interface*]

*interface*

**ethernet** *unit/port*

*unit* - Unit identifier. (Range: 1)

*port* - Port number. (Range: 1-12)

**port-channel** *channel-id* (Range: 1-12)

### Command Mode

Privileged Exec

### Example

```
Console#show ipv6 nd rguard 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

**show ipv6 neighbors** [**vlan** *vlan-id* | *ipv6-address*]

*vlan-id* - VLAN ID (Range: 1-4093)

*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:

```

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 VLAN
FE80::2E0:CFF:FE9C:CA10 4        00-E0-0C-9C-CA-10  R    1
Console#

```

**Table 173: show ipv6 neighbors - display description**

| Field           | Description  |
|-----------------|--|
| IPv6 Address    | IPv6 address of neighbor   |
| Age             | The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent." |
| Link-layer Addr | Physical layer MAC address.  |

**Table 173: show ipv6 neighbors - display description** (Continued)

| Field | Description  |
|-------|--|
| State | <p>The following states are used for dynamic entries:</p> <p>I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.</p> <p>I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293).</p> <p>R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.</p> <p>S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.</p> <p>D (Delay) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.</p> <p>P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.</p> <p>U (Unknown) - Unknown state.</p> <p>The following states are used for static entries:</p> <p>I1 (Incomplete)-The interface for this entry is down.</p> <p>R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.</p> <p>P2 (Permanent) - Indicates a static entry.</p> |
| VLAN  | VLAN interface from which the address was reached.   |

## 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 174: ND Snooping Commands**

| Command   | Function   | Mode |
|---|--|------|
| <code>ipv6 nd snooping</code>                                 | Enables ND snooping globally or on a specified VLAN or range of VLANs  | GC   |
| <code>ipv6 nd snooping auto-detect</code>                     | Enables automatic validation of binding table entries by periodically sending NS messages and awaiting NA replies  | GC   |
| <code>ipv6 nd snooping auto-detect retransmit count</code>    | Sets the number of times to send an NS message to determine if a binding is still valid  | GC   |
| <code>ipv6 nd snooping auto-detect retransmit interval</code> | Sets the interval between sending NS messages to determine if a binding is still valid   | GC   |
| <code>ipv6 nd snooping prefix timeout</code>                  | Sets the time to wait for an RA message before deleting an entry in the prefix table   | GC   |
| <code>ipv6 nd snooping max-binding</code>                     | Sets the maximum number of address entries which can be bound to a port  | IC   |
| <code>ipv6 nd snooping trust</code>                           | 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 | IC   |
| <code>clear ipv6 nd snooping binding</code>                   | Clears all entries in the address binding table  | PE   |
| <code>clear ipv6 nd snooping prefix</code>                    | Clears all entries in the prefix table   | PE   |
| <code>show ipv6 nd snooping</code>                            | Shows configuration settings for ND snooping   | PE   |
| <code>show ipv6 nd snooping binding</code>                    | Shows entries in the binding table   | PE   |
| <code>show ipv6 nd snooping prefix</code>                     | Show entries in the prefix table   | PE   |

**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: 1-4093)

*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 if 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* – The number of times to send an NS message to determine if a client still exists. (Range: 1-5)

#### 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 3 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

### Example

```
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

```

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

```

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: 1-4093)

#### 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#
```

# Section III

## Appendices

This section provides additional information and includes these items:

- ◆ [“Troubleshooting” on page 861](#)
- ◆ [“License Information” on page 863](#)





# Troubleshooting

## Problems Accessing the Management Interface

Table 175: Troubleshooting Chart

| Symptom   | Action   |
|---|--|
| Cannot connect using Telnet, web browser, or SNMP software                    | <ul style="list-style-type: none"><li>◆ Be sure the switch is powered up.</li><li>◆ Check network cabling between the management station and the switch.</li><li>◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled.</li><li>◆ 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.</li><li>◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.</li><li>◆ 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.</li><li>◆ 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.</li></ul> |
| Cannot connect using Secure Shell   | <ul style="list-style-type: none"><li>◆ 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.</li><li>◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station.</li><li>◆ 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.</li><li>◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.</li><li>◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).</li></ul>   |
| Cannot access the on-board configuration program via a serial port connection | <ul style="list-style-type: none"><li>◆ 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 115200 bps.</li><li>◆ Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.</li></ul>  |
| Forgot or lost the password   | <ul style="list-style-type: none"><li>◆ Contact your local distributor.</li></ul>  |

## 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
:
```



---

# License Information

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

---

# 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.

**CFM** Connectivity Fault Management provides fault monitoring for end-to-end connections within a designated service area by using continuity check messages which can detect faults in maintenance points, fault verification through loop back messages, and fault isolation with link trace messages.

**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.
- DNS** Domain Name Service. A system used for translating host names for network nodes into IP addresses.
- DSCP** 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.
- EAPOL** 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.
- ERPS** Ethernet Ring Protection Switching can be used to increase the availability and robustness of Ethernet rings, such as those used in Metropolitan Area Networks (MAN). ERPS provides Layer 2 loop avoidance and fast re-convergence in Layer 2 ring topologies, supporting up to 255 nodes in the ring structure. It can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist within the Ethernet ring.
- EUI** 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.
- GARP** 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.

- GMRP** 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.
- GVRP** 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.
- ICMP** 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.
- 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 a simple tree that uses IGMP Proxy.

**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** 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 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 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.

**Private VLANs** Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

**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 or backup 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.

---

# Command List

## A

aaa accounting dot1x 228  
aaa accounting exec 229  
aaa accounting update 230  
aaa authorization exec 231  
aaa group server 232  
absolute 156  
access-list arp 363  
access-list ip 344  
access-list ipv6 350  
access-list mac 358  
accounting dot1x 233  
accounting exec 233  
alias 371  
arp timeout 821  
authentication enable 218  
authentication login 219  
authorization exec 234  
auto-traffic-control 435  
auto-traffic-control action 435  
auto-traffic-control alarm-clear-threshold 436  
auto-traffic-control alarm-fire-threshold 437  
auto-traffic-control apply-timer 433  
auto-traffic-control auto-control-release 438  
auto-traffic-control control-release 439  
auto-traffic-control release-timer 434

## B

banner configure 93  
banner configure company 94  
banner configure dc-power-info 95  
banner configure department 95  
banner configure equipment-info 96  
banner configure equipment-location 97  
banner configure ip-lan 97  
banner configure ip-number 98  
banner configure manager-info 99  
banner configure mux 99  
banner configure note 100  
boot system 114  
bridge-ext gvrp 522  
bundle 589

## C

calendar set 154  
capabilities 372  
channel-group 406  
class 589

class-map 584  
clear access-list hardware counters 365  
clear arp-cache 822  
clear counters 379  
clear dns cache 794  
clear efm oam counters 782  
clear efm oam event-log 782  
clear erps statistics 511  
clear ethernet cfm ais mpid 747  
clear ethernet cfm errors 759  
clear ethernet cfm linktrace-cache 768  
clear ethernet cfm maintenance-points remote 758  
clear host 795  
clear ip dhcp snooping binding 315  
clear ip dhcp snooping database flash 315  
clear ip igmp snooping groups dynamic 621  
clear ip igmp snooping statistics 622  
clear ipv6 mld snooping groups dynamic 650  
clear ipv6 mld snooping statistics 651  
clear ipv6 nd snooping binding 856  
clear ipv6 nd snooping prefix 856  
clear ipv6 neighbors 848  
clear ipv6 traffic 840  
clear log 140  
clear mac-address-table dynamic 455  
clear mrv groups dynamic 676  
clear mrv statistics 676  
clear mvr6 groups dynamic 699  
clear mvr6 statistics 699  
clear network-access mac-address-table 295  
clear pppoe intermediate-agent statistics 275  
clock summer-time (date) 149  
clock summer-time (predefined) 151  
clock summer-time (recurring) 152  
clock timezone 153  
cluster 169  
cluster commander 170  
cluster ip-pool 171  
cluster member 171  
configure 87  
control-vlan 492  
copy 115

## D

databits 126  
delete 118  
delete public-key 247  
description 585  
description 373

## Command List

dir 119  
disable 88  
discard 374  
disconnect 133  
dos-protection echo-charge 332  
dos-protection smurf 332  
dos-protection tcp-flooding 333  
dos-protection tcp-null-scan 333  
dos-protection tcp-syn-fin-scan 334  
dos-protection tcp-udp-port-zero 334  
dos-protection tcp-xmas-scan 335  
dos-protection udp-flooding 335  
dos-protection win-nuke 336  
dot1q-tunnel system-tunnel-control 538  
dot1x default 253  
dot1x eapol-pass-through 254  
dot1x identity profile 261  
dot1x intrusion-action 255  
dot1x max-reauth-req 255  
dot1x max-req 256  
dot1x max-start 262  
dot1x operation-mode 256  
dot1x pae supplicant 262  
dot1x port-control 257  
dot1x re-authenticate 261  
dot1x re-authentication 258  
dot1x system-auth-control 254  
dot1x timeout auth-period 263  
dot1x timeout held-period 264  
dot1x timeout quiet-period 258  
dot1x timeout re-authperiod 259  
dot1x timeout start-period 264  
dot1x timeout supp-timeout 259  
dot1x timeout tx-period 260

## E

efm oam 778  
efm oam critical-link-event 778  
efm oam link-monitor frame 779  
efm oam link-monitor frame threshold 780  
efm oam link-monitor frame window 780  
efm oam mode 781  
efm oam remote-loopback 783  
efm oam remote-loopback test 784  
enable 493  
enable 85  
enable password 216  
end 89  
erps 491  
erps clear 511  
erps domain 491  
erps forced-switch 512  
erps manual-switch 514  
ethernet cfm ais level 738  
ethernet cfm ais ma 739  
ethernet cfm ais period 740  
ethernet cfm ais suppress alarm 740  
ethernet cfm cc enable 756

ethernet cfm cc ma interval 755  
ethernet cfm delay-measure two-way 775  
ethernet cfm domain 741  
ethernet cfm enable 743  
ethernet cfm linktrace 767  
ethernet cfm linktrace cache 764  
ethernet cfm linktrace cache hold-time 765  
ethernet cfm linktrace cache size 766  
ethernet cfm loopback 770  
ethernet cfm mep 746  
ethernet cfm mep crosscheck 763  
ethernet cfm mep crosscheck start-delay 761  
ethernet cfm port-enable 747  
exec-timeout 127  
exit 89

## F

flowcontrol 374

## G

garp timer 523  
guard-timer 494

## H

history 375  
holdoff-timer 494  
hostname 92

## I

interface 370  
interface vlan 529  
ip access-group 348  
ip address 814  
ip arp inspection 323  
ip arp inspection filter 324  
ip arp inspection limit 327  
ip arp inspection log-buffer logs 325  
ip arp inspection trust 328  
ip arp inspection validate 326  
ip arp inspection vlan 326  
ip default-gateway 816  
ip dhcp client class-id 801  
ip dhcp dynamic-provision 800  
ip dhcp relay information option 808  
ip dhcp relay information policy 811  
ip dhcp relay server 807  
ip dhcp restart client 803  
ip dhcp snooping 305  
ip dhcp snooping database flash 315  
ip dhcp snooping information option 307  
ip dhcp snooping information option circuit-id 312  
ip dhcp snooping information option encode no-subtype 308  
ip dhcp snooping information option remote-id 309  
ip dhcp snooping information policy 310

ip dhcp snooping trust 313  
 ip dhcp snooping verify mac-address 311  
 ip dhcp snooping vlan 311  
 ip domain-list 789  
 ip domain-lookup 790  
 ip domain-name 791  
 ip host 792  
 ip http port 236  
 ip http secure-port 237  
 ip http secure-server 238  
 ip http server 237  
 ip igmp authentication 633  
 ip igmp filter (Global Configuration) 630  
 ip igmp filter (Interface Configuration) 634  
 ip igmp max-groups 635  
 ip igmp max-groups action 636  
 ip igmp profile 630  
 ip igmp rate-limit 609  
 ip igmp rate-limit 631  
 ip igmp snooping 605  
 ip igmp snooping priority 606  
 ip igmp snooping proxy-reporting 607  
 ip igmp snooping querier 607  
 ip igmp snooping router-alert-option-check 608  
 ip igmp snooping router-port-expire-time 609  
 ip igmp snooping tcn-flood 610  
 ip igmp snooping tcn-query-solicit 611  
 ip igmp snooping unregistered-data-flood 612  
 ip igmp snooping unsolicited-report-interval 612  
 ip igmp snooping version 613  
 ip igmp snooping version-exclusive 614  
 ip igmp snooping vlan general-query-suppression 614  
 ip igmp snooping vlan last-memb-query-count 616  
 ip igmp snooping vlan last-memb-query-intvl 616  
 ip igmp snooping vlan mrd 617  
 ip igmp snooping vlan mrouter 628  
 ip igmp snooping vlan proxy-address 618  
 ip igmp snooping vlan query-interval 619  
 ip igmp snooping vlan static 621  
 ip igmp snooping vlan immediate-leave 615  
 ip igmp snooping vlan query-resp-intvl 620  
 ip multicast-data-drop 636  
 ip name-server 793  
 ip source-guard 319  
 ip source-guard binding 317  
 ip source-guard max-binding 320  
 ip ssh authentication-retries 245  
 ip ssh crypto host-key generate 248  
 ip ssh crypto zeroize 249  
 ip ssh save host-key 249  
 ip ssh server 245  
 ip ssh server-key size 246  
 ip ssh timeout 247  
 ip telnet max-sessions 240  
 ip telnet port 240  
 ip telnet server 241  
 ip tftp retry 123  
 ip tftp timeout 124  
 ipv6 access-group 356  
 ipv6 address 825  
 ipv6 address autoconfig 826  
 ipv6 address eui-64 828  
 ipv6 address link-local 829  
 ipv6 default-gateway 824  
 ipv6 dhcp client rapid-commit vlan 804  
 ipv6 dhcp restart client vlan 804  
 ipv6 enable 831  
 ipv6 hop-limit 843  
 ipv6 host 794  
 ipv6 mld filter (Global Configuration) 655  
 ipv6 mld filter (Interface Configuration) 658  
 ipv6 mld max-groups 658  
 ipv6 mld max-groups action 659  
 ipv6 mld profile 656  
 ipv6 mld query-drop 660  
 ipv6 mld snooping 642  
 ipv6 mld snooping proxy-reporting 643  
 ipv6 mld snooping querier 643  
 ipv6 mld snooping query-interval 644  
 ipv6 mld snooping query-max-response-time 644  
 ipv6 mld snooping robustness 645  
 ipv6 mld snooping router-port-expire-time 646  
 ipv6 mld snooping unknown-multicast mode 646  
 ipv6 mld snooping unsolicited-report-interval 647  
 ipv6 mld snooping version 648  
 ipv6 mld snooping vlan immediate-leave 648  
 ipv6 mld snooping vlan mrouter 649  
 ipv6 mld snooping vlan static 650  
 ipv6 mtu 832  
 ipv6 multicast-data-drop 660  
 ipv6 nd dad attempts 844  
 ipv6 nd ns-interval 845  
 ipv6 nd rguard 846  
 ipv6 nd reachable-time 847  
 ipv6 nd snooping 851  
 ipv6 nd snooping auto-detect 853  
 ipv6 nd snooping auto-detect retransmit count 853  
 ipv6 nd snooping auto-detect retransmit interval 854  
 ipv6 nd snooping max-binding 855  
 ipv6 nd snooping prefix timeout 854  
 ipv6 nd snooping trust 855  
  
**J**  
 jumbo frame 112  
  
**L**  
 l2protocol-tunnel tunnel-dmac 544  
 lacp 406  
 lacp admin-key (Ethernet Interface) 408  
 lacp admin-key (Port Channel) 411  
 lacp port-priority 409  
 lacp system-priority 410  
 lacp timeout 411  
 line 125  
 lldp 713

## Command List

lldp admin-status 717  
lldp basic-tlv management-ip-address 717  
lldp basic-tlv port-description 718  
lldp basic-tlv system-capabilities 718  
lldp basic-tlv system-description 719  
lldp basic-tlv system-name 719  
lldp dot1-tlv proto-ident 720  
lldp dot1-tlv proto-vid 720  
lldp dot1-tlv pvid 721  
lldp dot1-tlv vlan-name 721  
lldp dot3-tlv link-agg 722  
lldp dot3-tlv mac-phy 722  
lldp dot3-tlv max-frame 723  
lldp holdtime-multiplier 713  
lldp med-fast-start-count 714  
lldp med-location civic-addr 724  
lldp med-notification 725  
lldp med-tlv inventory 726  
lldp med-tlv location 727  
lldp med-tlv med-cap 727  
lldp med-tlv network-policy 728  
lldp notification 728  
lldp notification-interval 714  
lldp refresh-interval 715  
lldp reinit-delay 715  
lldp tx-delay 716  
logging facility 136  
logging history 137  
logging host 138  
logging on 138  
logging sendmail 143  
logging sendmail destination-email 145  
logging sendmail host 143  
logging sendmail level 144  
logging sendmail source-email 145  
logging trap 139  
login 128

## M

ma index name 744  
ma index name-format 745  
mac access-group 361  
mac-address-table aging-time 453  
mac-address-table static 454  
mac-authentication intrusion-action 294  
mac-authentication max-mac-count 295  
mac-authentication reauth-time 287  
mac-vlan 558  
major-domain 495  
management 268  
match 586  
max-hops 468  
media-type 376  
meg-level 496  
memory 196  
mep archive-hold-time 758  
mep crosscheck mpid 762  
mep fault-notify alarm-time 771

mep fault-notify lowest-priority 772  
mep fault-notify reset-time 773  
mep-monitor 497  
mst priority 469  
mst vlan 469  
mvr 665  
mvr associated-profile 666  
mvr domain 666  
mvr immediate-leave 673  
mvr priority 667  
mvr profile 667  
mvr proxy-query-interval 668  
mvr proxy-switching 669  
mvr robustness-value 670  
mvr source-port-mode dynamic 671  
mvr type 674  
mvr upstream-source-ip 671  
mvr vlan 672  
mvr vlan group 675  
mvr6 associated-profile 688  
mvr6 domain 689  
mvr6 immediate-leave 696  
mvr6 priority 690  
mvr6 profile 690  
mvr6 proxy-query-interval 691  
mvr6 proxy-switching 692  
mvr6 robustness-value 693  
mvr6 source-port-mode dynamic 694  
mvr6 type 697  
mvr6 upstream-source-ip 694  
mvr6 vlan 695  
mvr6 vlan group 698

## N

name 470  
negotiation 376  
network-access aging 285  
network-access dynamic-qos 287  
network-access dynamic-vlan 288  
network-access guest-vlan 289  
network-access link-detection 290  
network-access link-detection link-down 290  
network-access link-detection link-up 291  
network-access link-detection link-up-down 291  
network-access mac-filter 286  
network-access max-mac-count 292  
network-access mode mac-authentication 293  
network-access port-mac-filter 294  
nlm 193  
no rspan session 425  
node-id 498  
non-erps-dev-protect 499  
non-revertive 500

## P

parity 129  
password 129

password-thresh 130  
 periodic 157  
 permit, deny 632  
 permit, deny 657  
 permit, deny (ARP ACL) 364  
 permit, deny (Extended IPv4 ACL) 346  
 permit, deny (Extended IPv6 ACL) 353  
 permit, deny (MAC ACL) 359  
 permit, deny (Standard IP ACL) 345  
 permit, deny (Standard IPv6 ACL) 351  
 ping 820  
 ping6 840  
 police flow 591  
 police srtcm-color 592  
 police trtcm-color 595  
 policy-map 588  
 port channel load-balance 404  
 port monitor 417  
 port security 280  
 power-save 401  
 pppoe intermediate-agent 270  
 pppoe intermediate-agent format-type 271  
 pppoe intermediate-agent port-enable 272  
 pppoe intermediate-agent port-format-type 273  
 pppoe intermediate-agent trust 274  
 pppoe intermediate-agent vendor-tag strip 274  
 priority 597  
 process cpu 197  
 process cpu guard 198  
 prompt 83  
 propagate-tc 504  
 protocol-vlan protocol-group (Configuring Groups)  
     552  
 protocol-vlan protocol-group (Configuring Interfaces)  
     552

## Q

qos map cos-dscp 572  
 qos map dscp-cos 574  
 qos map dscp-mutation 575  
 qos map phb-queue 576  
 qos map trust-mode 577  
 queue mode 568  
 queue weight 569  
 quit 86

## R

radius-server acct-port 220  
 radius-server auth-port 221  
 radius-server host 221  
 radius-server key 222  
 radius-server retransmit 223  
 radius-server timeout 223  
 range 632  
 range 657  
 raps-def-mac 504  
 raps-without-vc 505

rate-limit 428  
 rcommand 172  
 reload (Global Configuration) 84  
 reload (Privileged Exec) 88  
 rename 587  
 revision 471  
 ring-port 507  
 rmon alarm 202  
 rmon collection history 204  
 rmon collection rmon1 205  
 rmon event 203  
 rpl neighbor 508  
 rpl owner 509  
 rspan destination 423  
 rspan remote vlan 424  
 rspan source 422

## S

server 232  
 service-policy 600  
 set cos 598  
 set ip dscp 598  
 set phb 599  
 sflow owner 209  
 sflow polling instance 211  
 sflow sampling instance 212  
 show access-group 366  
 show access-list 366  
 show access-list arp 365  
 show access-list tcam-utilization 102  
 show accounting 235  
 show alarm 102  
 show alarm-status 103  
 show arp 822  
 show auto-traffic-control 443  
 show auto-traffic-control interface 444  
 show banner 101  
 show bridge-ext 525  
 show cable-diagnostics 400  
 show calendar 155  
 show class-map 601  
 show cluster 172  
 show cluster candidates 173  
 show cluster members 173  
 show discard 380  
 show dns 795  
 show dns cache 796  
 show dos-protection 336  
 show dot1q-tunnel 543  
 show dot1x 265  
 show efm oam counters interface 785  
 show efm oam event-log interface 785  
 show efm oam remote-loopback interface 787  
 show efm oam status interface 787  
 show efm oam status remote interface 788  
 show erps 516  
 show ethernet cfm configuration 748  
 show ethernet cfm errors 760

## Command List

show ethernet cfm fault-notify-generator 774  
show ethernet cfm linktrace-cache 768  
show ethernet cfm ma 750  
show ethernet cfm maintenance-points local 751  
show ethernet cfm maintenance-points local detail mep 752  
show ethernet cfm maintenance-points remote crosscheck 764  
show ethernet cfm maintenance-points remote detail 753  
show ethernet cfm md 749  
show garp timer 526  
show gvrp configuration 526  
show history 86  
show hosts 796  
show interfaces brief 380  
show interfaces counters 381  
show interfaces history 385  
show interfaces protocol-vlan protocol-group 554  
show interfaces status 388  
show interfaces subnet-vlan 556  
show interfaces switchport 389  
show interfaces transceiver 397  
show interfaces transceiver-threshold 398  
show ip access-group 349  
show ip access-list 349  
show ip arp inspection configuration 329  
show ip arp inspection interface 329  
show ip arp inspection log 330  
show ip arp inspection statistics 330  
show ip arp inspection vlan 330  
show ip default-gateway 816  
show ip dhcp dynamic-provision 803  
show ip dhcp relay 812  
show ip dhcp snooping 316  
show ip dhcp snooping binding 316  
show ip igmp authentication 637  
show ip igmp filter 638  
show ip igmp profile 638  
show ip igmp rate-limit 639  
show ip igmp snooping 622  
show ip igmp snooping group 623  
show ip igmp snooping mrouter 624  
show ip igmp snooping statistics 625  
show ip igmp throttle interface 640  
show ip interface 817  
show ip multicast-data-drop 640  
show ip source-guard 321  
show ip source-guard binding 321  
show ip ssh 250  
show ip telnet 242  
show ip traffic 817  
show ipv6 access-group 356  
show ipv6 access-list 357  
show ipv6 default-gateway 833  
show ipv6 dhcp duid 806  
show ipv6 dhcp vlan 806  
show ipv6 interface 833  
show ipv6 mld filter 661  
show ipv6 mld profile 661  
show ipv6 mld query-drop 662  
show ipv6 mld snooping 651  
show ipv6 mld snooping group 652  
show ipv6 mld snooping group source-list 652  
show ipv6 mld snooping mrouter 653  
show ipv6 mld snooping statistics 654  
show ipv6 mld throttle interface 662  
show ipv6 mtu 835  
show ipv6 nd rguard 848  
show ipv6 nd snooping 857  
show ipv6 nd snooping binding 857  
show ipv6 nd snooping prefix 858  
show ipv6 neighbors 849  
show ipv6 traffic 836  
show l2protocol-tunnel 548  
show lacp 412  
show line 135  
show lldp config 729  
show lldp info local-device 730  
show lldp info remote-device 731  
show lldp info statistics 733  
show log 140  
show logging 141  
show logging sendmail 146  
show mac access-group 362  
show mac access-list 362  
show mac-address-table 455  
show mac-address-table aging-time 456  
show mac-address-table count 457  
show mac-vlan 558  
show management 269  
show memory 104  
show mvr 677  
show mvr associated-profile 678  
show mvr interface 678  
show mvr members 680  
show mvr profile 681  
show mvr statistics 682  
show mvr6 700  
show mvr6 associated-profile 701  
show mvr6 interface 702  
show mvr6 members 703  
show mvr6 profile 704  
show mvr6 statistics 704  
show network-access 296  
show network-access mac-address-table 297  
show network-access mac-filter 298  
show nlm oper-status 195  
show policy-map 601  
show policy-map interface 602  
show port monitor 419  
show port security 282  
show port-channel load-balance 416  
show power-save 402  
show pppoe intermediate-agent info 275  
show pppoe intermediate-agent statistics 276  
show process cpu 104  
show process cpu guard 105

show protocol-vlan protocol-group 553  
show public-key 250  
show qos map cos-dscp 578  
show qos map dscp-cos 578  
show qos map dscp-mutation 579  
show qos map phb-queue 580  
show qos map trust-mode 580  
show queue mode 571  
show queue weight 571  
show radius-server 224  
show reload 89  
show rmon alarms 206  
show rmon events 206  
show rmon history 206  
show rmon statistics 207  
show rspan 426  
show running-config 106  
show sflow 213  
show snmp 179  
show snmp engine-id 190  
show snmp group 191  
show snmp notify-filter 196  
show snmp user 192  
show snmp view 193  
show snmp-server enable port-traps 184  
show snmp sntp 149  
show spanning-tree 485  
show spanning-tree mst configuration 487  
show ssh 251  
show startup-config 108  
show subnet-vlan 557  
show synce 166  
show system 108  
show tacacs-server 227  
show tech-support 109  
show time-range 158  
show traffic-segmentation 341  
show udd 450  
show upgrade 123  
show users 110  
show version 110  
show vlan 536  
show vlan-translation 550  
show voice vlan 565  
show watchdog 111  
show web-auth 303  
show web-auth interface 303  
show web-auth summary 304  
shutdown 377  
silent-time 131  
snmp-server 177  
snmp-server community 178  
snmp-server contact 178  
snmp-server enable traps ethernet cfm cc 757  
snmp-server enable traps ethernet cfm crosscheck 761  
snmp-server enable port-traps atc broadcast-alarm-clear 439  
snmp-server enable port-traps atc broadcast-alarm-fire 440  
snmp-server enable port-traps atc broadcast-control-apply 440  
snmp-server enable port-traps atc broadcast-control-release 441  
snmp-server enable port-traps atc multicast-alarm-clear 441  
snmp-server enable port-traps atc multicast-alarm-fire 442  
snmp-server enable port-traps atc multicast-control-apply 442  
snmp-server enable port-traps atc multicast-control-release 443  
snmp-server enable port-traps mac-notification 184  
snmp-server enable traps 180  
snmp-server engine-id 185  
snmp-server group 186  
snmp-server host 182  
snmp-server location 179  
snmp-server notify-filter 194  
snmp-server user 187  
snmp-server view 189  
snmp client 147  
snmp poll 148  
snmp server 148  
spanning-tree 460  
spanning-tree bpdu-filter 471  
spanning-tree bpdu-guard 472  
spanning-tree cisco-prestandard 461  
spanning-tree cost 473  
spanning-tree edge-port 474  
spanning-tree forward-time 461  
spanning-tree hello-time 462  
spanning-tree link-type 475  
spanning-tree loopback-detection 476  
spanning-tree loopback-detection action 477  
spanning-tree loopback-detection release 483  
spanning-tree loopback-detection release-mode 477  
spanning-tree loopback-detection trap 478  
spanning-tree max-age 463  
spanning-tree mode 464  
spanning-tree mst configuration 466  
spanning-tree mst cost 479  
spanning-tree mst port-priority 480  
spanning-tree pathcost method 465  
spanning-tree port-bpdu-flooding 481  
spanning-tree port-priority 481  
spanning-tree priority 466  
spanning-tree protocol-migration 484  
spanning-tree root-guard 482  
spanning-tree spanning-disabled 483  
spanning-tree system-bpdu-flooding 467  
spanning-tree transmission-limit 467  
speed 131  
speed-duplex 378  
stopbits 132  
subnet-vlan 555  
switchport acceptable-frame-types 530

## Command List

switchport allowed vlan 531  
switchport dot1q-tunnel mode 539  
switchport dot1q-tunnel service match cvid 540  
switchport dot1q-tunnel tpid 542  
switchport forbidden vlan 524  
switchport gvrp 525  
switchport ingress-filtering 532  
switchport l2protocol-tunnel 547  
switchport mode 533  
switchport native vlan 534  
switchport packet-rate 429  
switchport priority default 570  
switchport vlan-translation 548  
switchport voice vlan priority 563  
switchport voice vlan rule 563  
switchport voice vlan security 564  
switchport voice vlan 562  
synce 159  
synce auto-clock-source-selecting 162  
synce clk-src-ssm 166  
synce ethernet 160  
synce ethernet clock-source 161  
synce force-clock-source-selecting 163  
synce ssm ethernet 164

## T

tacacs-server host 225  
tacacs-server key 225  
tacacs-server port 226  
tacacs-server retransmit 226  
tacacs-server timeout 227  
telnet (client) 241  
terminal 134  
test cable-diagnostics 399  
timeout login response 133  
time-range 155  
traceroute 818  
traceroute6 842  
traffic-segmentation 337  
traffic-segmentation session 338  
traffic-segmentation uplink/downlink 339  
traffic-segmentation uplink-to-uplink 340  
transceiver-monitor 391  
transceiver-threshold current 392  
transceiver-threshold rx-power 393  
transceiver-threshold temperature 394  
transceiver-threshold tx-power 395  
transceiver-threshold voltage 396  
transceiver-threshold-auto 391

## U

udld aggressive 448  
udld detection-interval 445  
udld message-interval 446  
udld port 449  
udld recovery 447  
udld recovery-interval 447

upgrade opcode auto 120  
upgrade opcode path 121  
upgrade opcode reload 122  
username 217

## V

version 509  
vlan 528  
vlan database 527  
vlan-trunking 534  
voice vlan 559  
voice vlan aging 560  
voice vlan mac-address 561

## W

watchdog software 111  
web-auth 301  
web-auth login-attempts 299  
web-auth quiet-period 300  
web-auth re-authenticate (IP) 302  
web-auth re-authenticate (Port) 302  
web-auth session-timeout 300  
web-auth system-auth-control 301  
whichboot 120  
wtr-timer 510

---

# Index

## Numerics

- 802.1Q tunnel 537
  - access 539
  - configuration, guidelines 537
  - configuration, limitations 538
  - CVID to SVID map 540
  - ethernet type 542
  - interface configuration 539–542
  - mode selection 539
  - status, configuring 538
  - TPID 542
  - uplink 539
- 802.1X
  - authenticator, configuring 255–261
  - global settings 253–254
  - port authentication 252, 254
  - port authentication accounting 233
  - supplicant, configuring 261–264

## A

- AAA
  - accounting 802.1X port settings 233
  - accounting exec command privileges 229
  - accounting exec settings 233
  - accounting summary 235
  - accounting update 230
  - accounting, configuring 228
  - authorization & accounting 228
  - authorization exec settings 231, 234
  - authorization method 234
  - authorization settings 231
  - authorization summary 235
  - RADIUS group settings 232
  - TACACS+ group settings 232
- acceptable frame type 530
- Access Control List *See* ACL
- ACL 343
  - ARP 363
  - binding to a port 348
  - IPv4 Extended 343, 346
  - IPv4 Standard 343, 345
  - IPv6 Extended 350, 353
  - IPv6 Standard 350, 351
  - MAC 358
  - time range 155

- address table 453
  - aging time 453
  - aging time, displaying 456
  - aging time, setting 453
- administrative users, displaying 110
- ARP
  - ACL 324
  - configuration 821
  - statistics 817
- ARP inspection 322
  - ACL filter 324
  - additional validation criteria 326
  - ARP ACL 363
  - enabling globally 323
  - enabling per VLAN 326
  - trusted ports 328
- ATC 149, 430, 850
  - control response 435
  - functional limitations 433
  - limiting traffic rates 432
  - shutting down a port 433
  - thresholds 436, 437
  - timers 433, 434
  - usage 432
- authentication
  - MAC address authentication 284, 293
  - MAC, configuring ports 284
  - network access 284, 293
  - public key 244
  - web 301
  - web authentication port information, displaying 303
  - web authentication, configuring ports 301
  - web authentication, re-authenticating address 302
  - web authentication, re-authenticating ports 302
  - web, configuring 301
- Automatic Traffic Control *See* ATC

## B

- BOOTP 814
- BPDU
  - filter 471
  - flooding when STA disabled on VLAN 481
  - flooding when STA globally disabled 467
  - guard 472
  - ignoring superior BPDUs 482

## Index

- selecting protocol based on message format 484
- shut down port on receipt 472
- bridge extension capabilities, displaying 525
- broadcast storm, threshold 429

## C

- cable diagnostics 399

- CDP

- discard 374

- CFM

- continuity check errors 759, 760
  - continuity check messages 499, 735, 755, 756
  - cross-check errors 757, 761, 763
  - cross-check message 735, 761, 763, 764
  - cross-check start delay 761
  - delay measure 775
  - domain service access point 742
  - fault isolation 735, 767
  - fault notification 735, 771, 772, 773
  - fault notification generator 772, 774
  - fault verification 735
  - link trace cache 765, 766, 768
  - link trace message 735, 764, 765, 767
  - loop back messages 735, 770
  - maintenance association 735, 744, 750
  - maintenance domain 735, 741, 749
  - maintenance end point 742, 746, 751
  - maintenance intermediate point 741, 742, 744, 751
  - maintenance level 741
  - maintenance point 735, 751
  - MEP archive 758
  - MEP direction 746
  - remote maintenance end point 752, 753, 758, 762
  - service instance 744
  - SNMP traps 757, 761

- class map

- description 585
  - DiffServ 584

- CLI

- command modes 74
  - showing commands 72

- clustering switches, management access 169

- command line interface *See* CLI

- committed burst size, QoS policy 591, 592, 595

- committed information rate, QoS policy 591, 592, 595

- community string 62, 178

- configuration file, DHCP download reference 59

- configuration files, restoring defaults 113

- configuration settings

- restoring 64, 113, 115
  - saving 64, 113, 115

- console port, required connections 50

- continuity check errors, CFM 759, 760

- continuity check messages, CFM 499, 735, 755, 756

- CoS 577

- configuring 567

- default mapping to internal values 573

- enabling 577

- layer 3/4 priorities 572

- priorities, mapping to internal values 572

- queue mapping 576

- queue mode 568

- queue weights, assigning 569

- CoS/CFI to PHB/drop precedence 572

- CPU

- status 104

- utilization, setting trap 197

- utilization, showing 104

- cross-check errors, CFM 757, 761, 763

- cross-check message, CFM 735, 761, 763, 764

- cross-check start delay, CFM 761

- CVLAN to SPVLAN map 540

## D

- Daylight Savings Time *See* summer time

- default IPv4 gateway, configuration 816

- default IPv6 gateway, configuration 824

- default priority, ingress port 570

- delay measure, CFM 775

- DHCP 814

- class identifier 801

- client 799, 814

- client identifier 801

- dynamic configuration 57

- option 82 information 808

- relay option 82 807, 808

- relay server 807

- DHCP snooping 304

- enabling 305

- global configuration 305

- information option 307

- information option policy 310

- information option, enabling 307

- policy selection 310

- specifying trusted interfaces 313

- subtype field 308

- verifying MAC addresses 311

- VLAN configuration 311

- DHCPv4 snooping

- information option 309

- information option, enabling 309

- option 82 information, circuit-id 312

- remote ID 309

- sub-length field 308

- sub-option format 308

- sub-type and sub-length, disabling 308

- subtype field 308

- DiffServ 583
    - binding policy to interface 600
    - bundle rate for class map groups 589
    - bundle, grouping class maps 589
    - class map 584, 589
    - class map, description 585
    - classifying QoS traffic 586
    - color aware, srTCM 592
    - color aware, trTCM 595
    - color blind, srTCM 592
    - color blind, trTCM 595
    - committed burst size 591, 592, 595
    - committed information rate 591, 592, 595
    - configuring 583
    - conforming traffic, configuring response 591, 592, 595
    - description 585
    - excess burst size 592
    - metering, configuring 591
    - peak burst size 595
    - peak information rate 595
    - policy map 588
    - policy map, description 585
    - priority, for traffic flow 597
    - QoS policy 588
    - service policy 600
    - setting CoS for matching packets 598
    - setting IP DSCP for matching packets 598
    - setting PHB for matching packets 599
    - single-rate, three-color meter 592
    - srTCM metering 592
    - traffic between CIR and BE, configuring response 592
    - traffic between CIR and PIR, configuring response 595
    - trTCM metering 595
    - two-rate, three-color meter 595
    - violating traffic, configuring response 591, 592, 595
  - DNS
    - default domain name 791
    - displaying the cache 796
    - domain name list 792
    - enabling lookup 790
    - name server list 793
    - static entries, IPv4 792
    - static entries, IPv6 794
  - Domain Name Service *See* DNS
  - domain service access point, CFM 742
  - downloading software 115
    - automatically 120
    - using FTP or TFTP 115
  - drop precedence
    - CoS priority mapping 572
    - DSCP ingress map 575
  - DSA encryption 248
  - DSCP 577
    - enabling 577
    - mapping to internal values 575
  - DSCP ingress map, drop precedence 575
  - DSCP to PHB/drop precedence 575
  - dynamic addresses
    - clearing 455
    - displaying 455
  - Dynamic Host Configuration Protocol *See* DHCP
  - dynamic QoS assignment 287
  - dynamic VLAN assignment 288
- E**
- edge port, STA 474
  - encryption
    - DSA 248
    - RSA 248
  - engine ID 185
  - ERPS
    - configuration guidelines 490
    - control VLAN 492
    - domain configuration 491
    - domain, enabling 493
    - global configuration 491
    - guard timer 494
    - hold-off timer 494
    - major domain 495
    - MEG level 496
    - node identifier 498
    - non-compliant device protection 499
    - propagate topology change 504
    - ring configuration 491
    - ring port, east interface 507
    - ring port, west interface 507
    - ring, enabling 493
    - RPL owner 509
    - secondary ring 495
    - status, displaying 516
    - wait-to-restore timer 510
    - WTR timer 510
  - Ethernet Ring Protection Switching *See* ERPS
  - event logging 136
  - excess burst size, QoS policy 592, 595
  - exec command privileges, accounting 229
  - exec settings
    - accounting 233
    - authorization 231, 234
- F**
- fault isolation, CFM 735, 767
  - fault notification generator, CFM 772, 774
  - fault notification, CFM 735, 771, 772, 773
  - fault verification, CFM 735

## Index

### firmware

- displaying version 110
- upgrading 115
- upgrading automatically 120
- upgrading with FTP or TFTP 115
- version, displaying 110

## G

- gateway, IPv4 default 816
- gateway, IPv6 default 824
- general security measures 279
- GNU license 863
- GVRP
  - enabling 522
  - global setting 522
  - interface configuration 525

## H

- hardware version, displaying 110
- HTTP, web server 237
- HTTPS 238
  - configuring 238
  - replacing SSL certificate 115
  - secure-site certificate 115
  - UDP port, configuring 237
- HTTPS, secure server 238

## I

- IEEE 802.1D 464
- IEEE 802.1s 464
- IEEE 802.1w 464
- IEEE 802.1X 252, 254
- IGMP
  - filter profiles, binding to interface 634
  - filter profiles, configuration 630
  - filter, interface configuration 634–636
  - filter, parameters 630–636
  - filtering & throttling 629
  - filtering & throttling, enabling 630
  - filtering & throttling, interface configuration 633–636
  - filtering & throttling, status 630
  - filtering, configuring profile 632
  - filtering, creating profile 630
  - filtering, group range 632
  - filtering, interface settings 634–636
  - groups, displaying 623
  - Layer 2 604
  - query 607
  - query, enabling 607
  - snooping 604
  - snooping & query, parameters 604
  - snooping, configuring 604

- snooping, enabling 605
- snooping, immediate leave 615
- IGMP snooping
  - configuring 604
  - enabling per interface 605
  - forwarding entries 623
  - immediate leave, status 615
  - interface attached to multicast router 624, 628
  - last member query count 616
  - last member query interval 616
  - proxy query address 618
  - proxy query interval 619
  - proxy query response interval 620
  - proxy reporting 607, 643
  - querier timeout 609
  - querier, enabling 607
  - router port expire time 609
  - static host interface 621
  - static multicast routing 628
  - static port assignment 621
  - static router interface 628
  - static router port, configuring 628
  - statistics, displaying 654
  - TCN flood 610
  - unregistered data flooding 612
  - version exclusive 614
  - version for interface, setting 613
  - version, setting 613
  - with proxy reporting 607, 643
- immediate leave, IGMP snooping 615
- immediate leave, MLD snooping 648
- importing user public keys 115, 118
- ingress filtering 532
- IP address
  - BOOTP/DHCP 803
  - setting 813
- IP filter, for management access 268
- IP source guard
  - configuring static entries 317
  - setting filter criteria 319
  - setting maximum bindings 320
- IP statistics 817
- IPv4 address
  - BOOTP/DHCP 814
  - dynamic configuration 57
  - manual configuration 54
  - setting 53, 814
- IPv6
  - displaying neighbors 849
  - duplicate address detection 844, 849
  - enabling 831
  - hop-limit, advertisements 843
  - MTU 832

- IPv6 address
  - dynamic configuration (global unicast) 58, 826
  - dynamic configuration (link-local) 58, 831
  - EUI format 828
  - EUI-64 setting 828
  - explicit configuration 831
  - global unicast 825
  - link-local 827, 829
  - manual configuration (global unicast) 54, 825
  - manual configuration (link-local) 54, 829
  - setting 53, 825
- IPv6 statistics 836
- J**
- jumbo frame 112
- K**
- key
  - private 242
  - public 242
  - user public, importing 115, 118
- key pair
  - host 242
  - host, generating 248
- L**
- LACP
  - configuration 403
  - group attributes, configuring 411
  - 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 616
- last member query interval, IGMP snooping 616
- layer 2, protocol tunnel 547
- license information, GNU 863
- Link Layer Discovery Protocol *See* LLDP
- link trace cache, CFM 765, 766, 768
- link trace message, CFM 735, 764, 765, 767
- link type, STA 475
- LLDP 711
  - device statistics details, displaying 733
  - device statistics, displaying 733
  - display device information 731
  - displaying remote information 731
  - interface attributes, configuring 717–728
  - local device information, displaying 730
  - message attributes 711
  - message statistics 733
  - remote information, displaying 731
  - remote port information, displaying 731
  - timing attributes, configuring 713–716
  - TLV, 802.1 720–721
  - TLV, 802.3 722–723
  - TLV, basic 717–719
  - TLV, management address 717
  - TLV, port description 718
  - TLV, system capabilities 718
  - TLV, system description 719
  - TLV, system name 719
- LLDP-MED 711
  - notification, status 725
  - TLV 711
  - TLV, inventory 726
  - TLV, location 724, 727
  - TLV, MED capabilities 727
  - TLV, network policy 728
- local engine ID 185
- logging
  - messages, displaying 140
  - syslog traps 139
  - to syslog servers 138
- logon authentication 215
  - encryption keys 222, 225
  - RADIUS client 220
  - RADIUS server 220
  - sequence 218, 219
  - settings 219
  - TACACS+ client 224
  - TACACS+ server 224
- logon authentication, settings 220, 224
- logon banner, configuring 92
- loop back messages, CFM 735, 770
- loopback detection, STA 476
- M**
- MAC address authentication 284
  - ports, configuring 284, 293
  - reauthentication 287
- MAC address, mirroring 417
- maintenance association, CFM 735, 744, 750
- maintenance domain, CFM 735, 741, 749
- maintenance end point, CFM 742, 746, 751
- maintenance intermediate point, CFM 741, 742, 744, 751
- maintenance level, CFM 741
- maintenance point, CFM 735, 751
- management access, filtering per address 268
- management access, IP filter 268
- matching class settings, classifying QoS traffic 586
- media-type 376
- memory
  - status 104
  - utilization, showing 104

## Index

- memory utilization, setting trap 196
  - MEP archive, CFM 758
  - mirror port
    - configuring 417
    - configuring local traffic 417
    - configuring remote traffic 420
  - MLD
    - filter profiles, configuration 656
    - filtering & throttling 655
    - filtering & throttling, configuring profile 657
    - filtering & throttling, creating profile 656
    - filtering & throttling, enabling 655
    - filtering & throttling, interface configuration 658–659
    - filtering & throttling, status 655
  - MLD snooping 641
    - configuring 641
    - enabling 642
    - immediate leave 648
    - immediate leave, status 648
    - multicast static router port 649
    - querier 643
    - querier, enabling 643
    - query interval 644
    - query, maximum response time 644
    - robustness value 645
    - static port assignment 650
    - static router port 649
    - unknown multicast, handling 646
    - version 648
  - MSTP 464
    - global settings, configuring 459
    - global settings, displaying 485
    - interface settings, configuring 460
    - interface settings, displaying 485
    - max hop count 468
    - path cost 479
    - region name 470
    - region revision 471
  - MTU for IPv6 832
  - multicast filtering 603
    - enabling IGMP snooping 605
    - enabling IGMP snooping per interface 605
    - enabling MLD snooping 642
    - router configuration 628
  - multicast groups 623
    - static 621, 623
  - multicast router discovery 617
  - multicast router port, displaying 624
  - multicast services
    - configuring 621
    - displaying 623
  - multicast static router port 628
    - configuring 628
    - configuring for MLD snooping 649
  - multicast storm, threshold 429
  - multicast, filtering and throttling 655
  - MVR
    - assigning static multicast groups 667, 675
    - configuring 664, 672
    - interface status, configuring 673–675
    - interface status, displaying 677
    - IP for control packets sent upstream 671
    - proxy switching 669
    - receiver groups, displaying 680
    - robust value for proxy switching 670
    - setting interface type 674
    - setting multicast domain 666
    - setting multicast groups 665, 667
    - setting multicast priority 667, 690
    - specifying a domain 666
    - specifying a VLAN 665, 672
    - specifying priority 667, 690
    - static binding 667, 675
    - static binding, group to port 675
    - statistics, displaying 682
    - using immediate leave 673
  - MVR6
    - assigning static multicast groups 690, 698
    - configuring 687, 695
    - interface status, configuring 696–698
    - interface status, displaying 702
    - IP for control packets sent upstream 694
    - proxy switching 692
    - receiver groups, displaying 703
    - robust value for proxy switching 693
    - setting interface type 697
    - setting multicast domain 689
    - setting multicast groups 690
    - specifying a domain 689
    - specifying a VLAN 695
    - static binding 690, 698
    - static binding, group to port 698
    - statistics, displaying 704
    - using immediate leave 696
- ## N
- ND snooping
    - automatic validation 853–854
    - enabling 851
    - max bindings 855
    - trusted interface 855
  - Neighbor Discovery Snooping *See* ND snooping
  - network access
    - authentication 284
    - dynamic QoS assignment 287
    - dynamic VLAN assignment 288
    - guest VLAN 289
    - MAC address filter 286

- port configuration 293
- reauthentication 287
- secure MAC information 297, 298

## O

### OAM

- active mode 781
- displaying settings and status 785–788
- enabling on switch ports 778
- errored frame link events 779–780
- event log, displaying 785
- message statistics, displaying 785
- mode selection 781
- passive mode 781
- remote device information, displaying 788
- remote loop back test 784
- setting to active mode 781
- setting to passive mode 781

Operations, Administration and Maintenance *See* OAM

## P

- password, line 129
- passwords 52, 216
  - administrator setting 217
- path cost 473
  - method 465
  - STA 465, 473
- peak burst size, QoS policy 595
- peak information rate, QoS policy 595
- per-hop behavior, DSCP ingress map 575
- PHB/drop precedence to CoS/CFI 574
- policy map
  - description 585
  - DiffServ 588
- port authentication 252, 254
- port priority
  - configuring 567
  - default ingress 570
  - STA 480, 481
- port security, configuring 280
- ports
  - autonegotiation 376
  - broadcast storm threshold 429
  - capabilities 372
  - configuring 369
  - discard CDP/PVST 374
  - duplex mode 378
  - flow control 374
  - forced selection on combo ports 376
  - mirroring 417
  - mirroring local traffic 417
  - mirroring remote traffic 420
  - multicast storm threshold 429

- speed 378
- statistics 381
- transceiver threshold, trap 391
- unknown unicast storm threshold 429
- power savings
  - configuring 401
  - enabling per port 401
- PPPoE 270–276
- priority, default port ingress 570
- private key 242
- problems, troubleshooting 861
- protocol migration 484
- protocol tunnel, layer 2 547
- protocol VLANs 550
  - configuring 550
  - configuring groups 552
  - configuring interfaces 552
  - group configuration 552
  - interface configuration 552
- proxy query address, IGMP snooping 618
- proxy query interval, IGMP snooping 619
- proxy query response interval, IGMP snooping 620
- proxy reporting, IGMP snooping 607, 643
- public key 242
- PVID, port native VLAN 534
- PVST, discard 374

## Q

- QoS 583
  - configuration guidelines 584
  - configuring 583
  - CoS/CFI to PHB/drop precedence 572
  - DSCP to PHB/drop precedence 575
  - dynamic assignment 287
  - matching class settings 586
  - PHB to queue 576
  - PHB/drop precedence to CoS/CFI 574
  - selecting DSCP, CoS 577
- QoS policy
  - committed burst size 591, 592, 595
  - excess burst size 592
  - peak burst size 595
  - srTCM 592
  - srTCM police meter 592
  - trTCM 595
  - trTCM police meter 595
- QoS policy, committed information rate 591, 592, 595
- QoS policy, peak information rate 595
- queue mode, setting 568
- queue weight, assigning to CoS 569

## Index

### R

#### RADIUS

- logon authentication 220
- settings 220

#### rate limit

- port 428
- setting 427

remote engine ID 185

remote logging 139

remote maintenance end point, CFM 752, 753, 758, 762

Remote Monitoring *See* RMON

rename, DiffServ 587

restarting the system 84, 88, 89

- at scheduled times 84

#### RMON 201

- alarm, displaying settings 206
- alarm, setting thresholds 202
- commands 201
- event settings, displaying 206
- response to alarm setting 203
- statistics history, collection 204
- statistics history, displaying 206
- statistics, collection 205
- statistics, displaying 207

root guard 482

RSA encryption 248

#### RSTP 464

- global settings, configuring 464
- global settings, displaying 485
- interface settings, configuring 471–483
- interface settings, displaying 485

running configuration files, displaying 106

### S

secure shell 242

- configuration 243

security, general measures 279

serial port, configuring 125

service instance, CFM 744

#### sFlow

- destination 210
- owner 209
- polling period 211
- sampling period 212
- timeout 210

#### SMTP

- event handling 142
- sending log events 142

#### SNMP 175

- community string 178
- enabling traps 180
- enabling traps, mac-address changes 184
- filtering IP addresses 268

global settings, configuring 177

mac address traps 180, 184

trap manager 182

traps, CFM 761

SNMP traps, CFM 757

SNMPv3 185–187

engine ID 185

engine identifier, local 185

engine identifier, remote 185

groups 186

local users, configuring 187

remote users, configuring 187

user configuration 187

views 189

#### SNTP

setting the system clock 147–149

specifying servers 148

#### software

displaying version 110

downloading 115

version, displaying 110

#### srTCM

police meter 592

QoS policy 592

#### SSH 242

authentication retries 245

configuring 243

downloading public keys for clients 115, 118

generating host key pair 248

server, configuring 245

timeout 247

#### STA 459

BPDU filter 471

BPDU flooding 481

BPDU shutdown 472

cisco-prestandard, setting compatibility 461

detecting loopbacks 476

edge port 474

forward delay 461

global settings, configuring 460–467

global settings, displaying 485

hello time 462

interface settings, configuring 471–483

interface settings, displaying 485

link type 475

loopback detection 476

maximum age 463

MSTP interface settings, configuring 479, 480

MSTP path cost 479

path cost 465, 473

path cost method 465

port priority 480, 481

port/trunk loopback detection 476

protocol migration 484

- transmission limit 467
- startup files
  - creating 115
  - displaying 108, 120
  - setting 114
- static addresses, setting 454
- statistics
  - ARP 817
  - history for port 385
  - history for trunk 385
  - ICMP 817
  - IP 817
  - port 381
  - TCP 817
  - UDP 817
  - VLAN 381
- STP 464
  - Also see* STA
- summary, accounting 235
- summer time, setting 149–152
- switch clustering, for management 168
- switch settings
  - restoring 113
  - saving 113
- SyncE
  - automatic clock source selection 162
  - clock source selection 161
  - clock source selection, forced 163
  - clock source selection, SSM 166
  - enabling on compatible ports 159, 160
  - SSM, enabling 164
  - Synchronization Status Messages (SSM) 164
- Synchronous Ethernet 158
- Synchronous Ethernet *See* SyncE
- system clock
  - setting 146
  - setting manually 154
  - setting the time zone 153
  - setting with SNTP 147–149
  - summer time 149–152
- system logs 138
- system software, downloading from server 115

## T

- TACACS+
  - logon authentication 224
  - settings 224
- TCN
  - flood 610
  - general query solicitation 611
- Telnet
  - configuring 239
  - server, enabling 241
- Telnet client 241

- telnet connection, configuring 125
- terminal, configuration settings 134
- TFTP
  - retry count 123
  - timeout 124
- time range, ACL 155
- time zone, setting 153
- time, setting 146
- TPID 542
- traffic segmentation 337
  - assigning ports 337, 338, 339
  - enabling 337, 338, 339
  - sessions, assigning ports 337, 338, 339
  - sessions, creating 337, 338, 339
- transceiver thresholds
  - displaying 398
- trap manager 62, 182
- troubleshooting 861
- trTCM
  - police meter 595
  - QoS policy 595
- trunk
  - configuration 403
  - LACP 403, 406
  - load balancing 404
  - static 406
- tunneling unknown VLANs, VLAN trunking 534

## U

- UDLD
  - configuration 445
  - interface settings 449
  - protocol intervals 445–447
- unidirectional link detection 445
- unknown unicast storm, threshold 429
- unregistered data flooding, IGMP snooping 612
- upgrading software 115, 120
- user account 216, 217
- user password 216, 217

## V

- VLAN trunking 534
- VLANs 521–565
  - 802.1Q tunnel mode 539
  - acceptable frame type 530
  - adding static members 531
  - basic information, displaying 525
  - configuring port members, by interface 530–534
  - creating 528
  - displaying port members 536
  - dynamic assignment 288
  - egress mode 533
  - ingress filtering 532

---

## Index

- interface configuration 530–534
  - IP subnet-based 555
  - MAC-based 557
  - mirroring 417
  - port members, displaying 536
  - protocol 550
  - protocol, configuring 550
  - protocol, configuring groups 552
  - protocol, configuring interfaces 552
  - protocol, group configuration 552
  - protocol, interface configuration 552
  - PVID 534
  - statistics 381
  - tag swapping 548
  - translation, customer and service provider 548
  - tunneling unknown groups 534
  - voice 559
- voice VLANs 559
  - detecting VoIP devices 559
  - enabling for ports 562–564
  - identifying client devices 561
- VoIP traffic 559
  - ports, configuring 562–564
  - telephony OUI, configuring 561
  - voice VLAN, configuring 559
- VoIP, detecting devices 563

## W

- web authentication 301
  - address, re-authenticating 302
  - configuring 301
  - configuring ports 301
  - port information, displaying 303
  - ports, configuring 301
  - ports, re-authenticating 302

