Notes, Notices, and Cautions

**NOTE:** A NOTE indicates important information that helps you make better use of your computer.

**NOTICE:** A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

**CAUTION:** A CAUTION indicates a potential for property damage, personal injury, or death.

Information in this document is subject to change without notice. © 2006 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell, the DELL logo, and PowerConnect are trademarks of Dell Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Aug 2006       Rev. A01
5 Address Table Commands

bridge address ........................................... 77
bridge multicast filtering ............................... 78
bridge multicast address ............................... 78
bridge multicast forbidden address .................. 80
bridge multicast forward-all ......................... 81
bridge multicast forbidden forward-all ............. 81
bridge aging-time ........................................ 82
clear bridge ................................................ 83
port security ................................................. 84
port security routed secure-address ................. 85
show bridge address-table .............................. 85
show bridge address-table static ..................... 87
show bridge address-table count ...................... 88
show bridge multicast address-table ................. 89
show bridge multicast filtering ....................... 91
show ports security ....................................... 91
6 Clock

clock set .......................................................... 93
clock source .......................................................... 93
clock timezone .......................................................... 94
clock summer-time ...................................................... 95
sntp authentication-key ............................................. 96
sntp authenticate ...................................................... 97
sntp trusted-key ...................................................... 98
sntp client poll timer ............................................... 98
sntp broadcast client enable ...................................... 99
sntp anycast client enable ......................................... 100
sntp client enable (interface) ...................................... 100
sntp unicast client enable .......................................... 101
sntp unicast client poll .............................................. 102
sntp server ........................................................... 102
show clock ........................................................... 103
show sntp configuration ............................................ 105
show sntp status ...................................................... 106

7 Configuration and Image Files

delete startup-config .............................................. 109
copy ................................................................. 109
boot system ........................................................... 112
show running-config ................................................ 113
show startup-config ................................................ 114
show backup-config ................................................ 116
show bootvar ........................................................ 118
8 Ethernet Configuration Commands

- interface ethernet ................................................. 119
- interface range ethernet ........................................ 119
- shutdown .......................................................... 120
- description ......................................................... 121
- speed .............................................................. 121
- duplex ............................................................. 122
- negotiation ......................................................... 123
- flowcontrol ......................................................... 123
- mdix ............................................................... 124
- back-pressure ...................................................... 125
- port jumbo-frame .................................................. 126
- clear counters ...................................................... 126
- set interface active ............................................... 127
- show interfaces configuration ................................. 127
- show interfaces status ........................................... 129
- show interfaces description ..................................... 131
- show interfaces counters ........................................ 132
- show ports jumbo-frame ......................................... 136
- port storm-control include-multicast ....................... 137
- port storm-control broadcast enable ......................... 137
- port storm-control broadcast rate ........................... 138
- show ports storm-control ....................................... 139

9 GVRP Commands

- gvrp enable (global) .............................................. 141
- gvrp enable (interface) .......................................... 141
**10  IGMP Snooping Commands**

- ip igmp snooping (Global) .................................................. 149
- ip igmp snooping (Interface) ............................................ 149
- ip igmp snooping mrouter .................................................. 150
- ip igmp snooping host-time-out ........................................ 150
- ip igmp snooping mrouter-time-out .................................... 151
- ip igmp snooping leave-time-out ....................................... 152
- show ip igmp snooping mrouter .......................................... 153
- show ip igmp snooping interface ........................................ 153
- show ip igmp snooping groups ........................................... 154

**11  IP Addressing Commands**

- clear host dhcp ............................................................. 157
- ip address ................................................................. 157
- ip address dhcp ............................................................ 158
- ip default-gateway ......................................................... 159
- show ip interface .......................................................... 160
- arp .................................................................................. 161
- arp timeout .................................................................... 162
clear arp-cache .................................................... 162
show arp ........................................................ 163
ip domain-lookup ............................................. 164
ip domain-name .............................................. 164
ip name-server ............................................... 165
ip host .......................................................... 165
clear host ..................................................... 166
show hosts ..................................................... 167

12 LACP Commands
lacp system-priority ......................................... 169
lacp port-priority ............................................ 169
lacp timeout ................................................... 170
show lacp ethernet .......................................... 171
show lacp port-channel ................................. 171

13 Line Commands
line .............................................................. 173
speed ............................................................ 173
autobaud ........................................................ 174
exec-timeout .................................................. 174
show line ....................................................... 175
terminal history ............................................. 176
terminal history size ...................................... 176

14 LLDP Commands
lldp enable (global) ........................................... 179
Syntax ......................................................... 179
lldp enable (interface) ........................................ 179
............................................................... lldp timer 180
........................................................................ lldp reinit-delay 181
lldp tx-delay ...................................................... 182
lldp optional-tlv ................................................. 183
lldp management-address ..................................... 183
clear lldp rx ....................................................... 184
show lldp configuration ........................................ 185
show lldp local .................................................... 185
show lldp neighbors ............................................. 186

15 Management ACL
management access-list ........................................ 189
permit (management) ........................................... 190
deny (management) ............................................. 191
management access-class ...................................... 192
show management access-list ................................ 193
show management access-class ................................ 193

16 PHY Diagnostics Commands
test copper-port tdr ........................................... 195
show copper-ports tdr .......................................... 195
show copper-ports cable-length ............................. 196
show fiber-ports optical-transceiver ....................... 197
17 Port Channel Commands

- interface port-channel ........................................... 201
- interface range port-channel ..................................... 201
- channel-group ......................................................... 202
- port channel load balance ........................................ 203
- show interfaces port-channel ...................................... 203

18 Port Monitor Commands

- port monitor ........................................................ 205
- show ports monitor ................................................. 206

19 QoS Commands

- qos ................................................................. 209
- show qos .......................................................... 209
- wrr-queue cos-map ............................................... 210
- wrr-queue bandwidth ............................................. 211
- priority-queue out num-of-queues ............................... 212
- show qos interface ............................................... 213
- qos map dscp-queue .............................................. 214
- qos trust (Global) ................................................. 215
- qos trust (Interface) .............................................. 216
- qos cos ............................................................ 216
- show qos map ...................................................... 217

20 Radius Commands

- radius-server host ................................................ 219
- radius-server key ................................................ 220
radius-server retransmit .............................................. 221
radius-server source-ip .............................................. 221
radius-server timeout .................................................. 222
radius-server deadtime ................................................. 223
show radius-servers .................................................... 223

21 RMON Commands

show rmon statistics ................................................... 225
rmon collection history ............................................... 227
show rmon collection history ......................................... 228
show rmon history ..................................................... 229
rmon alarm .............................................................. 232
show rmon alarm-table ............................................... 233
show rmon alarm ....................................................... 234
rmon event ............................................................. 236
show rmon events ....................................................... 237
show rmon log .......................................................... 238
rmon table-size ........................................................ 240

22 SNMP Commands

snmp-server community ............................................... 241
snmp-server view ....................................................... 242
snmp-server filter ...................................................... 243
snmp-server contact ................................................... 244
snmp-server location .................................................. 244
snmp-server enable traps ............................................. 245
snmp-server trap authentication .................................... 246
snmp-server host .......................................................... 246
snmp-server set .......................................................... 247
snmp-server group ......................................................... 248
snmp-server user .......................................................... 249
snmp-server v3-host ....................................................... 251
snmp-server engineID local ............................................. 252
show snmp engineid ...................................................... 253
show snmp ................................................................. 254
show snmp views ........................................................ 255
show snmp groups ......................................................... 256
show snmp filters ........................................................ 257
show snmp users .......................................................... 258

23  Spanning-Tree Commands

spanning-tree ............................................................. 261
spanning-tree mode ...................................................... 261
spanning-tree forward-time ............................................. 262
spanning-tree hello-time ............................................... 263
spanning-tree max-age .................................................. 264
spanning-tree priority ................................................... 265
spanning-tree disable .................................................... 265
spanning-tree cost ........................................................ 266
spanning-tree port-priority ............................................. 267
spanning-tree portfast ................................................... 267
spanning-tree link-type .................................................. 268
spanning-tree mst priority .............................................. 269
spanning-tree mst max-hops ......................................... 269
spanning-tree mst port-priority ........................................ 270
spanning-tree mst cost .................................................... 271
spanning-tree mst configuration ....................................... 271
instance (mst) ............................................................. 272
name (mst) ................................................................. 273
revision (mst) ............................................................. 273
show (mst) .................................................................. 274
exit (mst) .................................................................. 275
abort (mst) .................................................................. 275
spanning-tree pathcost method ....................................... 276
spanning-tree bpdu ......................................................... 276
clear spanning-tree detected-protocols ............................ 277
show spanning-tree ....................................................... 278
spanning-tree mst mstp-rstp ......................................... 290
Spanning-tree guard root ............................................... 291

24 SSH Commands
ip ssh port ................................................................ 293
ip ssh server ................................................................ 293
crypto key generate dsa ............................................... 294
crypto key generate rsa ............................................... 294
ip ssh pubkey-auth ..................................................... 295
crypto key pubkey-chain ssh ....................................... 296
user-key ................................................................. 296
key-string .............................................................. 297
show ip ssh .................................................................. 298
show crypto key mypubkey .......................................... 299
### Syslog Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging on</td>
<td>303</td>
</tr>
<tr>
<td>logging</td>
<td>303</td>
</tr>
<tr>
<td>logging console</td>
<td>304</td>
</tr>
<tr>
<td>logging buffered</td>
<td>305</td>
</tr>
<tr>
<td>logging buffered size</td>
<td>305</td>
</tr>
<tr>
<td>clear logging</td>
<td>306</td>
</tr>
<tr>
<td>logging file</td>
<td>307</td>
</tr>
<tr>
<td>clear logging file</td>
<td>307</td>
</tr>
<tr>
<td>show logging</td>
<td>308</td>
</tr>
<tr>
<td>show logging file</td>
<td>309</td>
</tr>
<tr>
<td>show syslog-servers</td>
<td>310</td>
</tr>
</tbody>
</table>

### System Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>313</td>
</tr>
<tr>
<td>traceroute</td>
<td>314</td>
</tr>
<tr>
<td>telnet</td>
<td>317</td>
</tr>
<tr>
<td>resume</td>
<td>320</td>
</tr>
<tr>
<td>reload</td>
<td>321</td>
</tr>
<tr>
<td>hostname</td>
<td>321</td>
</tr>
<tr>
<td>show users</td>
<td>322</td>
</tr>
<tr>
<td>show sessions</td>
<td>322</td>
</tr>
<tr>
<td>show system</td>
<td>323</td>
</tr>
</tbody>
</table>
show version .................................................. 324
asset-tag ..................................................... 325
show system id ............................................... 326

28 TACACS Commands

tacacs-server host ...................................... 327
tacacs-server key ....................................... 328
tacacs-server timeout .................................. 328
tacacs-server source-ip ................................. 329
show tacacs ............................................... 330

29 User Interface

enable ......................................................... 331
disable ....................................................... 331
login .......................................................... 332
configure .................................................... 332
exit(configuration) ...................................... 333
exit(EXEC) .................................................. 334
end ............................................................ 334
help .......................................................... 335
history ......................................................... 335
history size ................................................ 336
debug-mode ............................................... 336
show history ............................................... 337
show privilege ............................................ 338
30 VLAN Commands

   vlan database ........................................ 339
   vlan .................................................... 339
   default-vlan disable ................................... 340
   interface vlan .......................................... 340
   interface range vlan .................................... 341
   name ...................................................... 342
   switchport access vlan ................................. 342
   switchport trunk allowed vlan ......................... 343
   switchport trunk native vlan ........................... 344
   switchport general allowed vlan ....................... 344
   switchport general pvid ................................ 345
   switchport general ingress-filtering disable .......... 346
   switchport general acceptable-frame-type tagged-only 347
   switchport forbidden vlan ............................... 347
   map protocol protocols-group ............................ 348
   switchport general map protocols-group vlan .......... 349
   ip internal-usage-vlan .................................. 349
   show vlan ............................................... 350
   show vlan internal usage ................................ 351
   show vlan protocols-groups ............................. 352
   show interfaces switchport ............................. 353
   switchport mode ......................................... 354
   switchport customer vlan ............................... 355

31 Web Server

   ip http server ......................................... 357
ip http port .................................................. 357
ip https server .............................................. 358
ip https port .................................................. 358
crypto certificate generate .............................. 359
crypto certificate request ................................. 360
crypto certificate import .................................. 362
ip https certificate ........................................... 363
crypto certificate export pkcs12 ....................... 364
crypto certificate import pkcs12 ....................... 366
show crypto certificate mycertificate ............... 368
show ip http .................................................. 369
show ip https .................................................. 369

32  802.1x Commands
    aaa authentication dot1x .................................. 371
dot1x system-auto-control ............................... 372
dot1x port-control .......................................... 372
dot1x re-authentication .................................... 373
dot1x timeout re-authperiod ............................. 374
dot1x re-authenticate ....................................... 374
dot1x timeout quiet-period .............................. 375
dot1x timeout tx-period .................................... 376
dot1x max-req ................................................ 377
dot1x timeout supp-timeout .............................. 377
dot1x timeout server-timeout ............................ 378
show dot1x .................................................. 379
show dot1x users ............................................ 381
show dot1x statistics ........................................ 382
ADVANCED FEATURES ........................................ 384
dot1x auth-not-req ........................................ 384
dot1x multiple-hosts ....................................... 385
dot1x single-host-violation ............................... 385
show dot1x advanced ...................................... 386
Command Groups

Introduction

The Command Language Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphic User Interface (GUI) driven software application. By directly entering commands, you have greater configuration flexibility. The CLI is a basic command-line interpreter similar to the UNIX C shell.

A device can be configured and maintained by entering commands from the CLI, which is based solely on textual input and output with commands being entered from a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a VT100 terminal connected to the console port of the device or through a Telnet connection from a remote host.

This guide describes how the Command Line Interface (CLI) is structured, describes the command syntax, and describes the command functionality.

This guide also provides information for configuring the PowerConnect switch, details the procedures and provides configuration examples. Basic installation configuration is described in the User’s Guide and must be completed before using this document.

Command Groups

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

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Configures connection security including authorization and passwords.</td>
</tr>
<tr>
<td>Address Table</td>
<td>Configures bridging address tables.</td>
</tr>
<tr>
<td>Configuration and Image Files</td>
<td>Manages the device configuration files.</td>
</tr>
<tr>
<td>Clock</td>
<td>Configures clock commands on the device.</td>
</tr>
<tr>
<td>Ethernet Configuration</td>
<td>Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.</td>
</tr>
<tr>
<td>GVRP</td>
<td>Configures and displays GVRP configuration and information.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Configures IGMP snooping and displays IGMP configuration and IGMP information.</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>Configures and manages IP addresses on the device.</td>
</tr>
<tr>
<td>LACP</td>
<td>Configures and displays LACP information.</td>
</tr>
<tr>
<td>Line</td>
<td>Configures the console and remote Telnet connection.</td>
</tr>
<tr>
<td>LLDP</td>
<td>Configures and displays LLDP information.</td>
</tr>
<tr>
<td>Management ACL</td>
<td>Configures and displays management access-list information.</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PHY Diagnostics</td>
<td>Diagnoses and displays the interface status.</td>
</tr>
<tr>
<td>Port Channel</td>
<td>Configures and displays Port channel information.</td>
</tr>
<tr>
<td>Port Monitor</td>
<td>Monitors activity on specific target ports.</td>
</tr>
<tr>
<td>QoS</td>
<td>Configures and displays QoS information.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Configures and displays RADIUS information.</td>
</tr>
<tr>
<td>RMON</td>
<td>Displays RMON statistics.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Configures SNMP communities, traps and displays SNMP information.</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>Configures and reports on Spanning Tree protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Configures SSH authentication.</td>
</tr>
<tr>
<td>Syslog Commands</td>
<td>Manages and displays syslog messages.</td>
</tr>
<tr>
<td>System Management</td>
<td>Configures the device clock, name and authorized users.</td>
</tr>
<tr>
<td>TACACS</td>
<td>Configures TACACS commands</td>
</tr>
<tr>
<td>User Interface</td>
<td>Describes user commands used for entering CLI commands.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Configures VLANs and displays VLAN information.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Configures Web based access to the device.</td>
</tr>
<tr>
<td>802.1x</td>
<td>Configures commands related to 802.1x security protocol.</td>
</tr>
</tbody>
</table>
## AAA Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication login</td>
<td>Defines login authentication.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>aaa authentication enable</td>
<td>Defines authentication method lists for accessing higher privilege levels.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>login authentication</td>
<td>Specifies the login authentication method list for a remote telnet or console.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>enable authentication</td>
<td>Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.</td>
<td>Line Configuration</td>
</tr>
<tr>
<td>ip http authentication</td>
<td>Specifies authentication methods for http.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip https authentication</td>
<td>Specifies authentication methods for https.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show authentication methods</td>
<td>Displays information about the authentication methods.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password on a line.</td>
<td>Line Configuration</td>
</tr>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to normal and privilege levels.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>username</td>
<td>Establishes a username-based authentication system.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show users accounts</td>
<td>Displays information about the local user database.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>

## Address Table Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge address</td>
<td>Adds a static MAC-layer station source address to the bridge table.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>bridge multicast filtering</td>
<td>Enables filtering of multicast addresses.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>bridge multicast address</td>
<td>Registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>bridge multicast forbidden address</td>
<td>Forbids adding a specific multicast address to specific ports.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Access Mode</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>bridge multicast forward-all</td>
<td>Enables forwarding of all multicast frames on a port.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>bridge multicast forbidden forward-all</td>
<td>Enables forbidding forwarding of all multicast frames to a port.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>bridge aging-time</td>
<td>Sets the address table aging time.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clear bridge</td>
<td>Removes any learned entries from the forwarding database.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>port security</td>
<td>Disables new address learning on an interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>port security routed secure-address</td>
<td>Adds MAC-layer secure addresses to a routed port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show bridge address-table static</td>
<td>Displays statically created entries in the bridge-forwarding database.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show bridge address-table static count</td>
<td>Displays the number of addresses present in all or at a specific VLAN.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show bridge multicast address-table</td>
<td>Displays statically created entries in the bridge-forwarding database.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show bridge multicast filtering</td>
<td>Displays the multicast filtering configuration.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show ports security</td>
<td>Displays the port-lock status.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>

**Clock Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock set</td>
<td>Manually sets the system clock.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>clock source</td>
<td>Configures an external time source for the system clock.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>clock timezone</td>
<td>Sets the time zone for display purposes.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clock summer-time</td>
<td>Configures the system to automatically switch to summer time (daylight saving time).</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>sntp authentication-key</td>
<td>Defines an authentication key for Simple Network Time Protocol (SNTP).</td>
<td>Global Configuration</td>
</tr>
</tbody>
</table>
### Configuration and Image Files Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete startup-config</td>
<td>Deletes the startup-config file.</td>
<td>Privileged User</td>
</tr>
<tr>
<td>copy</td>
<td>Copies files from a source to a destination.</td>
<td>Privileged User</td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the system image that the device loads at startup.</td>
<td>Privileged User</td>
</tr>
</tbody>
</table>
### Ethernet Configuration Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the contents of the currently running configuration file.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the startup configuration file contents.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show backup-config</td>
<td>Displays the backup configuration file contents.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the active system image file that the device loads at startup.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface ethernet</td>
<td>Enters the interface configuration mode to configure an Ethernet type interface.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>interface range ethernet</td>
<td>Enters the interface configuration mode to configure multiple Ethernet type interfaces.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables interfaces.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>description</td>
<td>Adds a description to an interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>speed</td>
<td>Configures the speed of a given Ethernet interface when not using auto-negotiation.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>duplex</td>
<td>Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>negotiation</td>
<td>Enables auto-negotiation operation for the speed and duplex parameters of a given interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>flowcontrol</td>
<td>Configures the Flow Control on a given interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>mdix</td>
<td>Enables automatic crossover on a given interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>back-pressure</td>
<td>Enables Back Pressure on a given interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>port jumbo-frame</td>
<td>Enables jumbo frames for the device.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clear counters</td>
<td>Clears statistics on an interface.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>set interface active</td>
<td>Reactivates an interface that was suspended by the system.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show interfaces configuration</td>
<td>Displays the configuration for all configured interfaces.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays the status for all configured interfaces.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show interfaces description</td>
<td>Displays the description for all configured interfaces.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show interfaces counters</td>
<td>Displays traffic seen by the physical interface.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show ports jumbo-frame</td>
<td>Displays the jumbo frames configuration.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>port storm-control include-multicast</td>
<td>Enables the device to count multicast packets.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>port storm-control broadcast enable</td>
<td>Enables broadcast storm control.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>port storm-control broadcast rate</td>
<td>Configures the maximum broadcast rate.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show ports storm-control</td>
<td>Displays the storm control configuration.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>

### GVRP Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>gvrp enable (global)</td>
<td>Enables GVRP globally.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>gvrp enable (interface)</td>
<td>Enables GVRP on an interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>garp timer</td>
<td>Adjusts the GARP application join, leave, and leaveall GARP timer values.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>gvrp vlan-creation-forbid</td>
<td>Enables or disables dynamic VLAN creation.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>gvrp registration-forbid</td>
<td>De-registers all VLANs, and prevents dynamic VLAN registration on the port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>clear gvrp statistics</td>
<td>Clears all the GVRP statistics information.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show gvrp configuration</td>
<td>Displays GVRP configuration information.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show gvrp statistics</td>
<td>Displays GVRP statistics.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show gvrp error-statistics</td>
<td>Displays GVRP error statistics.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>
### IGMP Snooping Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>Enables Internet Group Management Protocol (IGMP) snooping.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>(Global)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping</td>
<td>Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>(Interface)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping mrouter</td>
<td>Enables automatic learning of multicast router ports in the context of a specific VLAN.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>ip igmp snooping host-time-out</td>
<td>Configures the host-time-out.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>ip igmp snooping mrouter-time-out</td>
<td>Configures the mrouter-time-out.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>ip igmp snooping leave-time-out</td>
<td>Configures the leave-time-out.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>Displays information on dynamically learned multicast router interfaces.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>mrouter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>Displays IGMP snooping configuration.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>Displays multicast groups learned by IGMP snooping.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>groups</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IP Addressing

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear host dhcp</td>
<td>Sets an IP address on the device.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>ip address</td>
<td>Sets an IP address</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>ip address dhcp</td>
<td>Acquires an IP address on an interface from the DHCP server.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>ip default-gateway</td>
<td>Defines a default gateway (router)</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays the usability status of interfaces configured for IP.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>arp</td>
<td>Adds a permanent entry in the ARP cache.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Access Mode</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>arp timeout</td>
<td>Configures how long an entry remains in the ARP cache.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clear arp-cache</td>
<td>Deletes all dynamic entries from the ARP cache.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show arp</td>
<td>Displays entries in the ARP table.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>ip domain-lookup</td>
<td>Enables the IP Domain Naming System (DNS)-based host name-to-address translation.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip domain-name</td>
<td>Defines a default domain name, that the software uses to complete unqualified host names.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip name-server</td>
<td>Sets the available name servers.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip host</td>
<td>Defines static host name-to-address mapping in the host cache.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clear host</td>
<td>Deletes entries from the host name-to-address cache</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show hosts</td>
<td>Displays the default domain name, a list of name server hosts, the static and cached list of host names and addresses.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

### LACP Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>lacp system-priority</td>
<td>Configures the system LACP priority.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>lacp port-priority</td>
<td>Configures the priority value for physical ports.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>lacp timeout</td>
<td>Assigns an administrative LACP timeout.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show lacp ethernet</td>
<td>Displays LACP information for Ethernet ports.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show lacp port-channel</td>
<td>Displays LACP information for a port-channel.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

### Line Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>Identifies a specific line for configuration and enters the line configuration command mode.</td>
<td>Global Configuration</td>
</tr>
</tbody>
</table>
### LLDP Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp enable (global)</td>
<td>Enables Link Layer Discovery Protocol.</td>
<td>Global configuration</td>
</tr>
<tr>
<td>lldp enable (interface)</td>
<td>Enables Link Layer Discovery Protocol (LLDP) on an interface.</td>
<td>Interface configuration (Ethernet)</td>
</tr>
<tr>
<td>lldp timer</td>
<td>Specifies how often the software sends Link Layer Discovery Protocol (LLDP) updates.</td>
<td>Global configuration</td>
</tr>
<tr>
<td>lldp hold-multiplier</td>
<td>Specifies the amount of time the receiving device should hold a Link Layer Discovery Protocol packet before discarding it.</td>
<td>Global configuration</td>
</tr>
<tr>
<td>lldp reinit-delay</td>
<td>Specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.</td>
<td>Global configuration</td>
</tr>
<tr>
<td>lldp tx-delay</td>
<td>Specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.</td>
<td>Global configuration</td>
</tr>
<tr>
<td>lldp optional-tlv</td>
<td>Specifies which optional TLVs from the basic set should be transmitted.</td>
<td>Interface configuration (Ethernet)</td>
</tr>
<tr>
<td>lldp management-address</td>
<td>Specifies the management address that would be advertised from an interface.</td>
<td>Interface configuration (Ethernet)</td>
</tr>
<tr>
<td>clear lldp rx</td>
<td>Restarts the LLDP RX state machine and clears the neighbors table.</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td>show lldp configuration</td>
<td>Displays the Link Layer Discovery Protocol (LLDP) configuration.</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td>show lldp local</td>
<td>Displays the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

### Command Groups

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>speed</td>
<td>Sets the line baud rate.</td>
</tr>
<tr>
<td>autobaud</td>
<td>Sets the line for automatic baud rate detection</td>
</tr>
<tr>
<td>exec-timeout</td>
<td>Configures the interval that the system waits until user input is detected.</td>
</tr>
<tr>
<td>show line</td>
<td>Displays line parameters.</td>
</tr>
</tbody>
</table>
### Management ACL Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>management access-list</td>
<td>Defines a management access-list, and enters the access-list for configuration.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>permit (management)</td>
<td>Defines a permit rule.</td>
<td>Management Access-level</td>
</tr>
<tr>
<td>deny (management)</td>
<td>Defines a deny rule.</td>
<td>Management Access-level</td>
</tr>
<tr>
<td>management access-class</td>
<td>Defines which management access-list is used.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show management access-list</td>
<td>Displays management access-lists.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show management access-class</td>
<td>Displays the active management access-list.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>

### PHY Diagnostics Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>test copper-port tdr</td>
<td>Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show copper-ports tdr</td>
<td>Displays the last TDR (Time Domain Reflectometry) tests on specified ports.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show copper-ports cable-length</td>
<td>Displays the estimated copper cable length attached to a port.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show fiber-ports optical-transceiver</td>
<td>Displays the optical transceiver diagnostics.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>
### Port Channel Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Enters the interface configuration mode of a specific port-channel.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>interface range port-channel</td>
<td>Enters the interface configuration mode to configure multiple port-channels.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>channel-group</td>
<td>Associates a port with a port-channel.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>port channel load balance</td>
<td>Configures the load balancing policy of the port channeling</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show interfaces port-channel</td>
<td>Displays port-channel information.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

### Port Monitor Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>port monitor</td>
<td>Starts a port monitoring session.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show ports monitor</td>
<td>Displays the port monitoring status.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

### QoS Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>Enables quality of service (QoS) on the device and enters QoS basic or advance mode.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show qos</td>
<td>Displays the QoS status.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>wrr-queue cos-map</td>
<td>Maps assigned CoS values to select one of the egress queues.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>wrr-queue bandwidth</td>
<td>Assigns Weighted Round Robin (WRR) weights to egress queues.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>priority-queue out num-of-queues</td>
<td>Enables the egress queues to be expedite queues.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show qos interface</td>
<td>Displays interface QoS data.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>qos map dscp-queue</td>
<td>Modifies the DSCP to CoS map.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Access Mode</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>qos trust (Global)</td>
<td>Configures the system to basic mode and the &quot;trust&quot; state.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>qos trust (Interface)</td>
<td>Enables each port trust state</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>qos cos</td>
<td>Configures the default port CoS value.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show qos map</td>
<td>Displays all the maps for QoS.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

### Radius Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-server host</td>
<td>Specifies a RADIUS server host.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>radius-server key</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>radius-server retransmit</td>
<td>Specifies the number of times the software searches the list of RADIUS server hosts.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>radius-server source-ip</td>
<td>Specifies the source IP address used for communication with RADIUS servers.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>radius-server timeout</td>
<td>Sets the interval for which a router waits for a server host to reply.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>radius-server deadtime</td>
<td>Improves RADIUS response times when servers are unavailable.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show radius-servers</td>
<td>Displays the RADIUS server settings.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>
### RMON Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon statistics</td>
<td>Displays RMON Ethernet Statistics.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>rmon collection history</td>
<td>Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show rmon collection history</td>
<td>Displays the requested history group configuration.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show rmon history</td>
<td>Displays RMON Ethernet Statistics history.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>rmon alarm</td>
<td>Configures alarm conditions.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show rmon alarm-table</td>
<td>Displays the alarms summary table.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show rmon alarm</td>
<td>Displays alarm configurations.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>rmon event</td>
<td>Configures a RMON event.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays the RMON event table.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show rmon log</td>
<td>Displays the RMON logging table.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>rmon table-size</td>
<td>Configures the maximum RMON tables sizes.</td>
<td>Global Configuration</td>
</tr>
</tbody>
</table>

### SNMP Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server community</td>
<td>Sets up the community access string to permit access to SNMP protocol.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>snmp-server view</td>
<td>Creates or update a view entry.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>snmp-server filter</td>
<td>Create or update a filter entry.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>snmp-server contact</td>
<td>Sets up a system contact.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>snmp-server location</td>
<td>Sets up the information on where the device is located.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>Enables the switch to send SNMP traps or SNMP notifications.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>snmp-server trap authentication</td>
<td>Enables the switch to send Simple Network Management Protocol traps when authentication failed.</td>
<td>Global Configuration</td>
</tr>
</tbody>
</table>
Spanning Tree Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree</td>
<td>Enables spanning tree functionality.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree mode</td>
<td>Configures the spanning tree protocol.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree forward-time</td>
<td>Configures the spanning tree bridge forward time.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree hello-time</td>
<td>Configures the spanning tree bridge Hello Time.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree max-age</td>
<td>Configures the spanning tree bridge maximum age.</td>
<td>Global Configuration</td>
</tr>
</tbody>
</table>

snmp-server host Specifies the recipient of Simple Network Management Protocol notification operation. Global Configuration

snmp-server set Sets SNMP MIB value by the CLI. Global Configuration

snmp-server group Configures a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views. Global Configuration

snmp-server user Configure a new SNMP Version 3 user. Global Configuration

snmp-server v3-host Specifies the recipient of Simple Network Management Protocol Version 3 notifications. Global Configuration

snmp-server engineID local Specifies the Simple Network Management Protocol (SNMP) engineID on the local device. Global Configuration

show snmp engineid Displays the ID of the local Simple Network Management Protocol (SNMP) engine. Privileged User EXEC

show snmp Displays the SNMP status.. Privileged User EXEC

show snmp views Displays the configuration of views. Privileged User EXEC

show snmp groups Displays the configuration of groups. Privileged User EXEC

show snmp filters Displays the configuration of filters. Privileged User EXEC

show snmp users Displays the configuration of groups. Privileged User EXEC
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Configuration Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree priority</td>
<td>Configures the spanning tree priority.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree disable</td>
<td>Disables spanning tree on a specific port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>spanning-tree cost</td>
<td>Configures the spanning tree path cost for a port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>spanning-tree port-priority</td>
<td>Configures port priority.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>spanning-tree portfast</td>
<td>Enables PortFast mode.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>spanning-tree mst priority</td>
<td>Configures the device priority for the specified spanning-tree instance.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree mst max-hops</td>
<td>Configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>spanning-tree mst port-priority</td>
<td>Configures port priority for the specified MST instance.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>spanning-tree mst cost</td>
<td>Configures the path cost for multiple spanning tree (MST) calculations.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>spanning-tree mst configuration</td>
<td>Enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>instance (mst)</td>
<td>Maps VLANs to an MST instance.</td>
<td>MST Configuration mode</td>
</tr>
<tr>
<td>name (mst)</td>
<td>Defines the configuration name.</td>
<td>MST Configuration mode</td>
</tr>
<tr>
<td>revision (mst)</td>
<td>Defines the configuration revision number.</td>
<td>MST Configuration mode</td>
</tr>
<tr>
<td>show (mst)</td>
<td>Displays the current or pending MST region configuration.</td>
<td>MST Configuration mode</td>
</tr>
<tr>
<td>exit (mst)</td>
<td>Exits the MST configuration mode and applies all configuration changes.</td>
<td>MST Configuration mode</td>
</tr>
<tr>
<td>abort (mst)</td>
<td>Exits the MST configuration mode without applying the configuration changes.</td>
<td>MST Configuration mode</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Access Mode</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>spanning-tree link-type</td>
<td>Overrides the default link-type setting.</td>
<td>Interface</td>
</tr>
<tr>
<td>spanning-tree pathcost</td>
<td>Sets the default path cost method.</td>
<td>Global</td>
</tr>
<tr>
<td>spanning-tree bpdu</td>
<td>Defines BPDU handling when spanning tree is disabled on an interface.</td>
<td>Global</td>
</tr>
<tr>
<td>clear spanning-tree</td>
<td>Restarts the protocol migration process on all interfaces or on the specified interface.</td>
<td>Privileged User</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>Displays spanning tree configuration.</td>
<td>Privileged User</td>
</tr>
<tr>
<td>spanning-tree mst mstp-rstp</td>
<td>Configure the switch to convert STP/RSTP packets to MSTP instances.</td>
<td>Global</td>
</tr>
<tr>
<td>Spanning-tree guard root</td>
<td>Enables root guard on all the spanning tree instances on that interface.</td>
<td>Interface</td>
</tr>
</tbody>
</table>

**SSH Commands**

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh port</td>
<td>Specifies the port to be used by the SSH server.</td>
<td>Global</td>
</tr>
<tr>
<td>ip ssh server</td>
<td>Enables the device to be configured from a SSH server.</td>
<td>Global</td>
</tr>
<tr>
<td>crypto key generate dsa</td>
<td>Generates DSA key pairs.</td>
<td>Global</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td>Generates RSA key pairs.</td>
<td>Global</td>
</tr>
<tr>
<td>ip ssh pubkey-auth</td>
<td>Enables public key authentication for incoming SSH sessions.</td>
<td>Global</td>
</tr>
<tr>
<td>crypto key pubkey-chain ssh</td>
<td>Enters SSH Public Key-chain configuration mode.</td>
<td>Global</td>
</tr>
<tr>
<td>user-key</td>
<td>Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.</td>
<td>SSH Public Key</td>
</tr>
<tr>
<td>key-string</td>
<td>Manually specifies a SSH public key.</td>
<td>SSH Public Key</td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Displays the SSH server configuration.</td>
<td>Privileged User</td>
</tr>
<tr>
<td>show crypto key mypubkey</td>
<td>Displays the SSH public keys stored on the device.</td>
<td>Privileged User</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Access Mode</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>show crypto key pubkey-chain ssh</td>
<td>Displays SSH public keys stored on the device.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>

### Syslog Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging on</td>
<td>Controls error messages logging.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>logging</td>
<td>Logs messages to a syslog server.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>logging console</td>
<td>Limits messages logged to the console based on severity.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>logging buffered</td>
<td>Limits syslog messages displayed from an internal buffer based on severity.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>logging buffered size</td>
<td>Changes the number of syslog messages stored in the internal buffer.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clear logging</td>
<td>Clears messages from the internal logging buffer.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>logging file</td>
<td>Limits syslog messages sent to the logging file based on severity.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>clear logging file</td>
<td>Clears messages from the logging file.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of logging and the syslog messages stored in the internal buffer.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show logging file</td>
<td>Displays the state of logging and the syslog messages stored in the logging file.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show syslog-servers</td>
<td>Displays the syslog servers settings.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>
## System Management Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>Sends ICMP echo request packets to another node on the network.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>traceroute</td>
<td>Discovers the routes that packets will actually take when traveling to their destination.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>telnet</td>
<td>Logs in to a host that supports Telnet.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>resume</td>
<td>Switches to another open Telnet session</td>
<td>User EXEC</td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the operating system</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies or modifies the device host name.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show users</td>
<td>Displays information about the active users.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show sessions</td>
<td>Lists the open Telnet sessions.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show system</td>
<td>Displays system information.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the system version information.</td>
<td>User EXEC</td>
</tr>
<tr>
<td>asset-tag</td>
<td>Specifies the device asset-tag.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show system id</td>
<td>Displays the service ID information.</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

## TACACS Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host</td>
<td>Specifies a TACACS+ host.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>Sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>tacacs-server source-ip</td>
<td>Specifies the source IP address that will be used for the communication with TACACS servers.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>tacacs-server timeout</td>
<td>Sets the timeout value.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>show tacacs</td>
<td>Displays configuration and statistics for a TACACS+ servers.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>
### User Interface Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enters the privileged EXEC mode.</td>
<td>All</td>
</tr>
<tr>
<td>disable</td>
<td>Returns to User EXEC mode.</td>
<td>All</td>
</tr>
<tr>
<td>login</td>
<td>Changes a login username.</td>
<td>All</td>
</tr>
<tr>
<td>configure</td>
<td>Enables the global configuration mode</td>
<td>All</td>
</tr>
<tr>
<td>exit(config)</td>
<td>Exits any configuration mode to the next highest mode in the CLI mode hierarchy.</td>
<td>All</td>
</tr>
<tr>
<td>exit(EXEC)</td>
<td>Closes an active terminal session by logging off the device.</td>
<td>All</td>
</tr>
<tr>
<td>end</td>
<td>Ends the current configuration session and returns to the previous command mode.</td>
<td>All</td>
</tr>
<tr>
<td>help</td>
<td>Displays a brief description of the help system.</td>
<td>All</td>
</tr>
<tr>
<td>history</td>
<td>Enables the command history function.</td>
<td>All</td>
</tr>
<tr>
<td>history size</td>
<td>Changes the command history buffer size for a particular line.</td>
<td>All</td>
</tr>
<tr>
<td>debug-mode</td>
<td>Switches the mode to debug.</td>
<td>All</td>
</tr>
<tr>
<td>show history</td>
<td>Lists the commands entered in the current session.</td>
<td>All</td>
</tr>
<tr>
<td>show privilege</td>
<td>Displays the current privilege level.</td>
<td>All</td>
</tr>
</tbody>
</table>

### VLAN Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan database</td>
<td>Enters the VLAN database configuration mode.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>vlan</td>
<td>Creates a VLAN.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>default-vlan disable</td>
<td>Disables the default VLAN functionality.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Enters the interface configuration (VLAN) mode.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>interface range vlan</td>
<td>Enters the interface configuration mode to configure multiple VLANs.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>name</td>
<td>Configures a name to a VLAN.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Mode</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><code>switchport access vlan</code></td>
<td>Configures the VLAN membership mode of a port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport access vlan</code></td>
<td>Configures the VLAN ID when the interface is in access mode.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport trunk allowed vlan</code></td>
<td>Adds or removes VLANs from a port in general mode.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport trunk native vlan</code></td>
<td>Defines the port as a member of the specified VLAN, and the VLAN ID is the &quot;port default VLAN ID (PVID)&quot;.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport general allowed vlan</code></td>
<td>Adds or removes VLANs from a general port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport general pvid</code></td>
<td>Configures the PVID when the interface is in general mode.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport general ingress-filtering disable</code></td>
<td>Disables port ingress filtering.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport general acceptable-frame-type tagged-only</code></td>
<td>Discards untagged frames at ingress.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>switchport forbidden vlan</code></td>
<td>Forbids adding specific VLANs to a port.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>map protocol protocols-group</code></td>
<td>Adds a special protocol to a named group of protocols, which may be used for protocol-based VLAN assignment.</td>
<td>VLAN Configuration</td>
</tr>
<tr>
<td><code>switchport general map protocols-group vlan</code></td>
<td>Sets a protocol-based classification rule.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>ip internal-usage-vlan</code></td>
<td>Reserves a VLAN as the internal usage VLAN of an interface.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td><code>show vlan</code></td>
<td>Displays VLAN information.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td><code>show vlan internal usage</code></td>
<td>Displays a list of VLANs being used internally by the switch.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td><code>show vlan protocols-groups</code></td>
<td>Displays protocols-groups information.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Displays switchport configuration.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td><code>switchport mode</code></td>
<td>Configures the VLAN membership mode of a port (Ethernet, port-channel)</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>switchport customer vlan</td>
<td>Sets the port's VLAN when the interface is in customer mode.</td>
<td>Interface configuration (Ethernet, port-channel)</td>
</tr>
</tbody>
</table>

## Web Server Commands

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip http server</td>
<td>Enables the device to be configured from a browser.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip http port</td>
<td>Specifies the TCP port for use by a web browser to configure the device.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip https port</td>
<td>Configures a TCP port for use by a secure web browser to configure the device.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip https server</td>
<td>Enables the device to be configured from a secured browser.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>crypto certificate generate</td>
<td>Generates a HTTPS certificate.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>crypto certificate request</td>
<td>Generates and displays certificate requests for HTTPS.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>crypto certificate import</td>
<td>Imports a certificate signed by Certification Authority for HTTPS.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>ip https certificate</td>
<td>Configures the active certificate for HTTPS.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>crypto certificate export pkcs12</td>
<td>Exports the certificate and the RSA keys within a PKCS12 file</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show ip http</td>
<td>Displays the HTTP server configuration.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show ip https</td>
<td>Displays the HTTPS server configuration.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show crypto certificate mycertificate</td>
<td>Displays the SSL certificates of the device</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>
# 802.1x Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication</td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>dot1x</td>
<td>Enables 802.1x globally.</td>
<td>Global Configuration</td>
</tr>
<tr>
<td>dot1x system-auto-control</td>
<td>Enables manual control of the authorization state of the port</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x re-authentication</td>
<td>Enables periodic re-authentication of the client.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x timeout re-authperiod</td>
<td>Sets the number of seconds between re-authentication attempts.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x re-authenticate</td>
<td>Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>dot1x timeout quiet-period</td>
<td>Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x timeout tx-period</td>
<td>Sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame, from the client, before resending the request.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x max-req</td>
<td>Sets the maximum number of times that the switch sends an EAP - request/identity frame to the client, before restarting the authentication process.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x timeout supp-timeout</td>
<td>Sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>dot1x timeout server-timeout</td>
<td>Sets the time for the retransmission of packets to the authentication server.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Allows multiple hosts on an 802.1X-authorized port, that has the dot1x port-control interface configuration command set to auto.</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>show dot1x users</td>
<td>Displays 802.1X statistics for the specified interface.</td>
<td>Privileged User EXEC</td>
</tr>
<tr>
<td>show dot1x statistics</td>
<td>Displays 802.1X statistics for the specified interface.</td>
<td>Privileged User EXEC</td>
</tr>
</tbody>
</table>
### Command Modes

#### GC (Global Configuration) Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication enable</td>
<td>Defines authentication method lists for accessing higher privilege levels.</td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>Defines login authentication.</td>
</tr>
<tr>
<td>aaa authentication dot1x</td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.</td>
</tr>
<tr>
<td>arp</td>
<td>Adds a permanent entry in the ARP cache.</td>
</tr>
<tr>
<td>arp timeout</td>
<td>Configures how long an entry remains in the ARP cache</td>
</tr>
<tr>
<td>asset-tag</td>
<td>Specifies the device asset-tag.</td>
</tr>
<tr>
<td>bridge aging-time</td>
<td>Sets the address table aging time.</td>
</tr>
<tr>
<td>bridge multicast filtering</td>
<td>Enables filtering of multicast addresses.</td>
</tr>
<tr>
<td>clock source</td>
<td>Configures an external time source for the system clock.</td>
</tr>
<tr>
<td>clock timezone</td>
<td>Sets the time zone for display purposes</td>
</tr>
<tr>
<td>clock summer-time</td>
<td>Configures the system to automatically switch to summer time (daylight saving time).</td>
</tr>
<tr>
<td>crypto certificate generate</td>
<td>Generates a HTTPS certificate.</td>
</tr>
<tr>
<td>crypto certificate import</td>
<td>Imports a certificate signed by Certification Authority for HTTPS.</td>
</tr>
<tr>
<td>crypto key generate dsa</td>
<td>Generates DSA key pairs.</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td>crypto key pubkey-chain ssh</td>
<td>Enters SSH Public Key-chain configuration mode.</td>
</tr>
<tr>
<td>dot1x system-auto-control</td>
<td>Enables 802.1x globally.</td>
</tr>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to normal and privilege levels.</td>
</tr>
<tr>
<td>end</td>
<td>Ends the current configuration session and returns to the previous command mode.</td>
</tr>
<tr>
<td>gvrp enable (global)</td>
<td>Enables GVRP globally.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies or modifies the device host name.</td>
</tr>
<tr>
<td>interface ethernet</td>
<td>Enters the interface configuration mode to configure an Ethernet type interface.</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Enters the interface configuration mode of a specific port-channel.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>interface range ethernet</code></td>
<td>Enters the interface configuration mode to configure multiple ethernet type interfaces.</td>
</tr>
<tr>
<td><code>interface range port-channel</code></td>
<td>Enters the interface configuration mode to configure multiple port-channels.</td>
</tr>
<tr>
<td><code>interface range vlan</code></td>
<td>Enters the interface configuration mode to configure multiple VLANs.</td>
</tr>
<tr>
<td><code>interface vlan</code></td>
<td>Enters the interface configuration (VLAN) mode.</td>
</tr>
<tr>
<td><code>ip default-gateway</code></td>
<td>Defines a default gateway.</td>
</tr>
<tr>
<td><code>ip domain-lookup</code></td>
<td>Enables the IP Domain Naming System (DNS)-based host name-to-address translation.</td>
</tr>
<tr>
<td><code>ip domain-name</code></td>
<td>Defines a default domain name, that the software uses to complete unqualified host names.</td>
</tr>
<tr>
<td><code>ip host</code></td>
<td>Defines static host name-to-address mapping in the host cache.</td>
</tr>
<tr>
<td><code>ip http authentication</code></td>
<td>Specifies authentication methods for http.</td>
</tr>
<tr>
<td><code>ip http port</code></td>
<td>Specifies the TCP port for use by a web browser to configure the device.</td>
</tr>
<tr>
<td><code>ip http server</code></td>
<td>Enables the device to be configured from a browser.</td>
</tr>
<tr>
<td><code>ip https authentication</code></td>
<td>Specifies authentication methods for https.</td>
</tr>
<tr>
<td><code>ip https certificate</code></td>
<td>Configures the active certificate for HTTPS. Use the no form of this command to return to default.</td>
</tr>
<tr>
<td><code>ip https server</code></td>
<td>Enables the device to be configured from a secured browser.</td>
</tr>
<tr>
<td><code>ip https port</code></td>
<td>Configures a TCP port for use by a secure web browser to configure the device.</td>
</tr>
<tr>
<td><code>ip igmp snooping (Global)</code></td>
<td>Enables Internet Group Management Protocol (IGMP) snooping.</td>
</tr>
<tr>
<td><code>ip name-server</code></td>
<td>Sets the available name servers.</td>
</tr>
<tr>
<td><code>ip ssh port</code></td>
<td>Specifies the port to be used by the SSH server.</td>
</tr>
<tr>
<td><code>ip ssh pubkey-auth</code></td>
<td>Enables public key authentication for incoming SSH sessions.</td>
</tr>
<tr>
<td><code>ip ssh server</code></td>
<td>Enables the device to be configured from a SSH server.</td>
</tr>
<tr>
<td><code>lacp system-priority</code></td>
<td>Configures the system LACP priority.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>Identifies a specific line for configuration and enters the line configuration command mode.</td>
</tr>
<tr>
<td><code>logging</code></td>
<td>Logs messages to a syslog server.</td>
</tr>
<tr>
<td><code>logging buffered</code></td>
<td>Limits syslog messages displayed from an internal buffer based on severity.</td>
</tr>
<tr>
<td><code>logging buffered size</code></td>
<td>Changes the number of syslog messages stored in the internal buffer.</td>
</tr>
<tr>
<td><code>logging console</code></td>
<td>Limits messages logged to the console based on severity.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>logging file</td>
<td>Limits syslog messages sent to the logging file based on severity.</td>
</tr>
<tr>
<td>logging on</td>
<td>Controls error messages logging.</td>
</tr>
<tr>
<td>login authentication</td>
<td>Specifies the login authentication method list for a remote telnet or console.</td>
</tr>
<tr>
<td>management access-class</td>
<td>Defines which management access-list is used.</td>
</tr>
<tr>
<td>management access-list</td>
<td>Defines a management access-list, and enters the access-list for configuration.</td>
</tr>
<tr>
<td>port jumbo-frame</td>
<td>Enables jumbo frames for the device.</td>
</tr>
<tr>
<td>port storm-control include-multicast</td>
<td>Enables the device to count multicast packets.</td>
</tr>
<tr>
<td>priority-queue out num-queue</td>
<td>Enables the egress queues to be expedite queues.</td>
</tr>
<tr>
<td>qos</td>
<td>Enables quality of service (QoS) on the device and enters QoS basic or advance mode.</td>
</tr>
<tr>
<td>qos map dscp-queue</td>
<td>Modifies the DSCP to CoS map.</td>
</tr>
<tr>
<td>qos trust (Global)</td>
<td>Configure the system to &quot;trust&quot; state.</td>
</tr>
<tr>
<td>radius-server deadtime</td>
<td>Improves RADIUS response times when servers are unavailable.</td>
</tr>
<tr>
<td>radius-server host</td>
<td>Specifies a RADIUS server host.</td>
</tr>
<tr>
<td>radius-server key</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
<tr>
<td>radius-server retransmit</td>
<td>Specifies the number of times the software searches the list of RADIUS server hosts.</td>
</tr>
<tr>
<td>radius-server source-ip</td>
<td>Specifies the source IP address used for communication with RADIUS servers.</td>
</tr>
<tr>
<td>radius-server timeout</td>
<td>Sets the interval for which a router waits for a server host to reply.</td>
</tr>
<tr>
<td>rmon alarm</td>
<td>Configures alarm conditions.</td>
</tr>
<tr>
<td>rmon event</td>
<td>Configures a RMON event.</td>
</tr>
<tr>
<td>rmon table-size</td>
<td>Configures the maximum RMON tables sizes.</td>
</tr>
<tr>
<td>snmp-server community</td>
<td>Sets up the community access string to permit access to SNMP protocol.</td>
</tr>
<tr>
<td>snmp-server contact</td>
<td>Sets up a system contact.</td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>Enables the switch to send SNMP traps or SNMP notifications.</td>
</tr>
<tr>
<td>snmp-server host</td>
<td>Specifies the recipient of Simple Network Management Protocol notification operation.</td>
</tr>
<tr>
<td>snmp-server location</td>
<td>Sets up the information on where the device is located.</td>
</tr>
</tbody>
</table>
Command Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>back-pressure</td>
<td>Enables Back Pressure on a given interface.</td>
</tr>
<tr>
<td>channel-group</td>
<td>Associates a port with a Port-channel.</td>
</tr>
<tr>
<td>clear host dhcp</td>
<td>Sets an IP address on the device.</td>
</tr>
<tr>
<td>description</td>
<td>Adds a description to an interface.</td>
</tr>
<tr>
<td>dot1x auth-not-req</td>
<td>Enables unauthorized users access to that VLAN</td>
</tr>
</tbody>
</table>

IC (Interface Configuration) Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server set</td>
<td>Sets SNMP MIB value by the CLI.</td>
</tr>
<tr>
<td>snmp-server trap authentication</td>
<td>Enables the switch to send Simple Network Management Protocol traps when authentication failed.</td>
</tr>
<tr>
<td>snmp authenticate</td>
<td>Enables the switch to send Simple Network Management Protocol traps when authentication failed.</td>
</tr>
<tr>
<td>sntp authenticate</td>
<td>Enables the switch to send Simple Network Management Protocol traps when authentication failed.</td>
</tr>
<tr>
<td>sntp authentication-key</td>
<td>Enables the switch to send Simple Network Management Protocol traps when authentication failed.</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Enables spanning tree functionality.</td>
</tr>
<tr>
<td>spanning-tree bpdu</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>spanning-tree forward-time</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>spanning-tree hello-time</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>spanning-tree max-age</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>spanning-tree mode</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>spanning-tree pathcost method</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>spanning-tree priority</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>tacacs-server source-ip</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>tacacs-server timeout</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>tacacs-server host</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>username</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>vlan database</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
<tr>
<td>wrr-queue cos-map</td>
<td>Enables BPDU handling when spanning tree is disabled on an interface.</td>
</tr>
</tbody>
</table>

www.dell.com | support.dell.com
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x max-req</code></td>
<td>Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client, before restarting the authentication process.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Allows multiple hosts on an 802.1X-authorized port, that has the dot1x port-control interface configuration command set to auto.</td>
</tr>
<tr>
<td><code>dot1x port-control</code></td>
<td>Enables manual control of the authorization state of the port.</td>
</tr>
<tr>
<td><code>dot1x re-authentication</code></td>
<td>Enables periodic re-authentication of the client.</td>
</tr>
<tr>
<td><code>dot1x single-host-violation</code></td>
<td>Configures the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface.</td>
</tr>
<tr>
<td><code>dot1x timeout quiet-period</code></td>
<td>Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange.</td>
</tr>
<tr>
<td><code>dot1x timeout re-authperiod</code></td>
<td>Sets the number of seconds between re-authentication attempts.</td>
</tr>
<tr>
<td><code>dot1x timeout server-timeout</code></td>
<td>Sets the time for the retransmission of packets to the authentication server.</td>
</tr>
<tr>
<td><code>dot1x timeout supp-timeout</code></td>
<td>Sets the time for the retransmission of an EAP-request frame to the client.</td>
</tr>
<tr>
<td><code>dot1x timeout tx-period</code></td>
<td>Sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame, from the client, before resending the request.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Sets the number of seconds that the switch waits for a response to an EAP request/identity frame, from the client, before resending the request.</td>
</tr>
<tr>
<td><code>duplex</code></td>
<td>Configures the full/half duplex operation of a given ethernet interface when not using auto-negotiation.</td>
</tr>
<tr>
<td><code>flowcontrol</code></td>
<td>Configures the Flow Control on a given interface.</td>
</tr>
<tr>
<td><code>garp timer</code></td>
<td>Adjusts the GARP application join, leave, and leavcall GARP timer values.</td>
</tr>
<tr>
<td><code>gvrp enable (interface)</code></td>
<td>Enables GVRP on an interface.</td>
</tr>
<tr>
<td><code>gvrp registration-forbid</code></td>
<td>De-registers all VLANs, and prevents dynamic VLAN registration on the port.</td>
</tr>
<tr>
<td><code>gvrp vlan-creation-forbid</code></td>
<td>Enables or disables dynamic VLAN creation.</td>
</tr>
<tr>
<td><code>ip address</code></td>
<td>Sets an IP address</td>
</tr>
<tr>
<td><code>ip address dhcp</code></td>
<td>Acquires an IP address on an interface from the DHCP server.</td>
</tr>
<tr>
<td><code>ip internal-usage-vlan</code></td>
<td>Reserves a VLAN as the internal usage VLAN of an interface.</td>
</tr>
<tr>
<td><code>lacp port-priority</code></td>
<td>Configures the priority value for physical ports.</td>
</tr>
<tr>
<td><code>lacp timeout</code></td>
<td>Assigns an administrative LACP timeout.</td>
</tr>
<tr>
<td><code>mdix</code></td>
<td>Enables automatic crossover on a given interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>Configures a name to a VLAN.</td>
</tr>
<tr>
<td><strong>negotiation</strong></td>
<td>Enables auto-negotiation operation for the speed and duplex parameters of a given interface.</td>
</tr>
<tr>
<td><strong>port monitor</strong></td>
<td>Starts a port monitoring session.</td>
</tr>
<tr>
<td><strong>port security</strong></td>
<td>Disables new address learning on an interface.</td>
</tr>
<tr>
<td><strong>port security routed secure-address</strong></td>
<td>Adds MAC-layer secure addresses to a routed port.</td>
</tr>
<tr>
<td><strong>port storm-control broadcast enable</strong></td>
<td>Enables broadcast storm control.</td>
</tr>
<tr>
<td><strong>port storm-control broadcast rate</strong></td>
<td>Configures the maximum broadcast rate.</td>
</tr>
<tr>
<td><strong>qos cos</strong></td>
<td>Configures the default port CoS value.</td>
</tr>
<tr>
<td><strong>qos trust (Interface)</strong></td>
<td>Enables each port trust state while the system is in basic mode.</td>
</tr>
<tr>
<td><strong>rmon collection history</strong></td>
<td>Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.</td>
</tr>
<tr>
<td><strong>shutdown</strong></td>
<td>Disables interfaces.</td>
</tr>
<tr>
<td><strong>snmp client enable (interface)</strong></td>
<td>Enables the Simple Network Time Protocol (SNTP) client on an interface.</td>
</tr>
<tr>
<td><strong>spanning-tree cost</strong></td>
<td>Configures the spanning tree path cost for a port.</td>
</tr>
<tr>
<td><strong>spanning-tree disable</strong></td>
<td>Disables spanning tree on a specific port.</td>
</tr>
<tr>
<td><strong>spanning-tree link-type</strong></td>
<td>Overrides the default link-type setting.</td>
</tr>
<tr>
<td><strong>spanning-tree portfast</strong></td>
<td>Enables PortFast mode.</td>
</tr>
<tr>
<td><strong>spanning-tree port-priority</strong></td>
<td>Configures port priority.</td>
</tr>
<tr>
<td><strong>speed</strong></td>
<td>Configures the speed of a given ethernet interface when not using auto-negotiation.</td>
</tr>
<tr>
<td><strong>qos map dscp-queue</strong></td>
<td>Defines the wrr-queue mechanism on an egress queue.</td>
</tr>
<tr>
<td><strong>wrr-queue bandwidth</strong></td>
<td>Assigns Weighted Round Robin (WRR) weights to egress queues.</td>
</tr>
</tbody>
</table>

**LC (Line Configuration) Mode**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>enable authentication</strong></td>
<td>Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.</td>
</tr>
<tr>
<td><strong>exec-timeout</strong></td>
<td>Configures the interval that the system waits until user input is detected.</td>
</tr>
<tr>
<td><strong>history</strong></td>
<td>Enables the command history function.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>history size</td>
<td>Changes the command history buffer size for a particular line.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password on a line.</td>
</tr>
<tr>
<td>autobaud</td>
<td>Sets the line for automatic baud rate detection.</td>
</tr>
<tr>
<td>speed</td>
<td>Sets the line baud rate.</td>
</tr>
</tbody>
</table>

### MA (Management Access-level) Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny (management)</td>
<td>Defines a deny rule.</td>
</tr>
<tr>
<td>permit (management)</td>
<td>Defines a permit rule.</td>
</tr>
</tbody>
</table>

### PE (Privileged User EXEC) Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x users</td>
<td>Displays 802.1X statistics for the specified interface.</td>
</tr>
<tr>
<td>boot system</td>
<td>Specifies the system image that the device loads at startup.</td>
</tr>
<tr>
<td>clear arp-cache</td>
<td>Deletes all dynamic entries from the ARP cache.</td>
</tr>
<tr>
<td>clear bridge</td>
<td>Removes any learned entries from the forwarding database.</td>
</tr>
<tr>
<td>clear gvrp statistics</td>
<td>Clears all the GVRP statistics information.</td>
</tr>
<tr>
<td>clear host</td>
<td>Deletes entries from the host name-to-address cache</td>
</tr>
<tr>
<td>clear host dhcp</td>
<td>Deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).</td>
</tr>
<tr>
<td>clear logging</td>
<td>Clears messages from the internal logging buffer.</td>
</tr>
<tr>
<td>clear logging file</td>
<td>Clears messages from the logging file</td>
</tr>
<tr>
<td>clear spanning-tree detected-protocols</td>
<td>Restarts the protocol migration process on all interfaces or on the specified interface.</td>
</tr>
<tr>
<td>clock set</td>
<td>Manually sets the system clock.</td>
</tr>
<tr>
<td>configure</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies files from a source to a destination.</td>
</tr>
<tr>
<td>crypto certificate request</td>
<td>Generates and displays certificate requests for HTTPS.</td>
</tr>
<tr>
<td>dot1x re-authenticate</td>
<td>Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.</td>
</tr>
<tr>
<td>login</td>
<td>Returns to User EXEC mode.</td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the operating system.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>set interface active</td>
<td>Reactivates an interface that was suspended by the system.</td>
</tr>
<tr>
<td>show arp</td>
<td>Displays entries in the ARP table.</td>
</tr>
<tr>
<td>show authentication methods</td>
<td>Displays information about the authentication methods.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Displays the active system image file that the device loads at startup.</td>
</tr>
<tr>
<td>show bridge address-table</td>
<td>Displays dynamically created entries in the bridge-forwarding database.</td>
</tr>
<tr>
<td>show bridge address-table count</td>
<td>Displays the number of addresses present in all VLANs or at specific VLAN.</td>
</tr>
<tr>
<td>show bridge multicast address-table</td>
<td>Displays statically created entries in the bridge-forwarding database.</td>
</tr>
<tr>
<td>show bridge multicast address-table</td>
<td>Displays multicast MAC address table information.</td>
</tr>
<tr>
<td>show bridge multicast filtering</td>
<td>Displays the multicast filtering configuration.</td>
</tr>
<tr>
<td>show copper-ports cable-length</td>
<td>Displays the estimated copper cable length attached to a port.</td>
</tr>
<tr>
<td>show copper-ports tdr</td>
<td>Displays the last TDR (Time Domain Reflectometry) tests on specified ports.</td>
</tr>
<tr>
<td>show crypto key mypubkey</td>
<td>Displays the SSH public keys stored on the device.</td>
</tr>
<tr>
<td>show crypto key pubkey-chain ssh</td>
<td>Displays SSH public keys stored on the device.</td>
</tr>
<tr>
<td>show crypto certificate mycertificate</td>
<td>Displays the SSL certificates of the device.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays 802.1X status for the switch or for the specified interface.</td>
</tr>
<tr>
<td>show dot1x advanced</td>
<td>Displays 802.1X enhanced features for the switch or for the specified interface.</td>
</tr>
<tr>
<td>show dot1x users</td>
<td>Displays 802.1X users for the switch.</td>
</tr>
<tr>
<td>show fiber-ports optical-transceiver</td>
<td>Displays the optical transceiver diagnostics.</td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Displays the SSH server configuration.</td>
</tr>
<tr>
<td>show lacp port-channel</td>
<td>Displays LACP information for a port-channel.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the state of logging and the syslog messages stored in the internal buffer.</td>
</tr>
<tr>
<td>show logging file</td>
<td>Displays the state of logging and the syslog messages stored in the logging file.</td>
</tr>
<tr>
<td>show management access-class</td>
<td>Displays the active management access-list.</td>
</tr>
<tr>
<td>show management access-list</td>
<td>Displays management access-lists.</td>
</tr>
<tr>
<td>show ports security</td>
<td>Displays the port-lock status.</td>
</tr>
</tbody>
</table>
show ports storm-control | Displays the storm control configuration.
show radius-servers | Displays the RADIUS server settings.
show running-config | Displays the contents of the currently running configuration file.
show snmp | Displays the SNMP status.
show spanning-tree | Displays spanning tree configuration.
show startup-config | Displays the startup configuration file contents.
show syslog-servers | Displays the syslog servers settings.
show tacacs | Displays configuration and statistics for a TACACS+ servers.
show users accounts | Displays information about the local user database.
test copper-port tdr | Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.

**SP (SSH Public Key) Mode**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-string</td>
<td>Manually specifies a SSH public key.</td>
</tr>
<tr>
<td>user-key</td>
<td>Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command</td>
</tr>
</tbody>
</table>

**UE (User EXEC) Mode**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters</td>
<td>Clears statistics on an interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Enters the privileged EXEC mode.</td>
</tr>
<tr>
<td>exit(EXEC)</td>
<td>Closes an active terminal session by logging off the device.</td>
</tr>
<tr>
<td>login</td>
<td>Changes a login username.</td>
</tr>
<tr>
<td>ping</td>
<td>Sends ICMP echo request packets to another node on the network.</td>
</tr>
<tr>
<td>show clock</td>
<td>Displays the time and date from the system clock.</td>
</tr>
<tr>
<td>show gvrp config</td>
<td>Displays GVRP configuration information.</td>
</tr>
<tr>
<td>show gvrp error-statistics</td>
<td>Displays GVRP error statistics.</td>
</tr>
<tr>
<td>clear gvrp stats</td>
<td>Displays GVRP statistics.</td>
</tr>
<tr>
<td>show history</td>
<td>Lists the commands entered in the current session.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show hosts</td>
<td>Displays the default domain name, a list of name server hosts, the static</td>
</tr>
<tr>
<td></td>
<td>and the cached list of host names and addresses.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the configuration for all configured interfaces.</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays traffic seen by the physical interface.</td>
</tr>
<tr>
<td>counters</td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the description for all configured interfaces.</td>
</tr>
<tr>
<td>description</td>
<td></td>
</tr>
<tr>
<td>port channel</td>
<td>Displays Port-channel information.</td>
</tr>
<tr>
<td>load balance</td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays the status for all configured interfaces.</td>
</tr>
<tr>
<td>status</td>
<td></td>
</tr>
<tr>
<td>show ip igmp</td>
<td>Displays multicast groups learned by IGMP snooping.</td>
</tr>
<tr>
<td>snooping groups</td>
<td></td>
</tr>
<tr>
<td>show ip igmp</td>
<td>Displays IGMP snooping configuration.</td>
</tr>
<tr>
<td>snooping interface</td>
<td></td>
</tr>
<tr>
<td>show ip igmp</td>
<td>Displays information on dynamically learned multicast router interfaces.</td>
</tr>
<tr>
<td>snooping mrouter</td>
<td></td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
<tr>
<td>show lacp ethernet</td>
<td>Displays LACP information for Ethernet ports.</td>
</tr>
<tr>
<td>show line</td>
<td>Displays line parameters.</td>
</tr>
<tr>
<td>show ports jumbo-frame</td>
<td>Displays the jumbo frames configuration.</td>
</tr>
<tr>
<td>show ports monitor</td>
<td>Displays the port monitoring status.</td>
</tr>
<tr>
<td>show privilege</td>
<td>Displays the current privilege level.</td>
</tr>
<tr>
<td>show qos</td>
<td>Displays the QoS status.</td>
</tr>
<tr>
<td>show qos interface</td>
<td>Assigns CoS values to select one of the egress queues.</td>
</tr>
<tr>
<td>show qos map</td>
<td>Displays all the maps for QoS.</td>
</tr>
<tr>
<td>show rmon alarm</td>
<td>Displays alarm configurations.</td>
</tr>
<tr>
<td>show rmon alarm-table</td>
<td>Displays the alarms summary table.</td>
</tr>
<tr>
<td>show rmon collection</td>
<td>Displays the requested history group configuration.</td>
</tr>
<tr>
<td>history</td>
<td></td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays the RMON event table.</td>
</tr>
<tr>
<td>show rmon history</td>
<td>Displays RMON Ethernet Statistics history.</td>
</tr>
<tr>
<td>show rmon log</td>
<td>Displays the RMON logging table.</td>
</tr>
<tr>
<td>show rmon statistics</td>
<td>Displays RMON Ethernet Statistics.</td>
</tr>
<tr>
<td>show system</td>
<td>Displays system information.</td>
</tr>
<tr>
<td>show system id</td>
<td>Displays the service id information.</td>
</tr>
<tr>
<td>show users</td>
<td>Displays information about the active users.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the system version information.</td>
</tr>
</tbody>
</table>
VC (VLAN Configuration) Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge address</td>
<td>Adds a static MAC-layer station source address to the bridge table.</td>
</tr>
<tr>
<td>bridge multicast address</td>
<td>Registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group.</td>
</tr>
<tr>
<td>bridge multicast forbidden address</td>
<td>Forbids adding a specific multicast address to specific ports.</td>
</tr>
<tr>
<td>bridge multicast forbidden forward-all</td>
<td>Enables forbidding forwarding of all multicast frames to a port.</td>
</tr>
<tr>
<td>bridge multicast forward-all</td>
<td>Enables forwarding of all multicast frames on a port.</td>
</tr>
<tr>
<td>ip igmp snooping (Interface)</td>
<td>Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.</td>
</tr>
<tr>
<td>ip igmp snooping host-time-out</td>
<td>Configures the host-time-out.</td>
</tr>
<tr>
<td>ip igmp snooping leave-time-out</td>
<td>Configures the leave-time-out.</td>
</tr>
<tr>
<td>show ip igmp snooping mrouter</td>
<td>Enables automatic learning of multicast router ports in the context of a specific VLAN.</td>
</tr>
<tr>
<td>ip igmp snooping mrouter-time-out</td>
<td>Configures the mrouter-time-out.</td>
</tr>
<tr>
<td>vlan</td>
<td>Creates a VLAN.</td>
</tr>
</tbody>
</table>
Using the CLI

This chapter describes how to start using the CLI and describes implemented command editing features to assist in using the CLI.

**CLI Command Modes**

**Introduction**

To assist in configuring devices, the CLI [Command Line Interface] is divided into different command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the system prompt (console prompt) displays a list of commands available for that particular command mode.

From each mode a specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: User EXEC mode, Privileged EXEC mode, Global Configuration mode, and Interface Configuration mode. The following figure illustrates the command mode access path.
When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands are available in User EXEC Mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged mode gives access to commands that are restricted on EXEC mode and provides access to the device Configuration mode.

The Global Configuration mode manages the device configuration on a global level.

The Interface Configuration mode configures specific interfaces in the device.

**User EXEC Mode**

After logging into the device, the user is automatically in User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the device "host name" followed by the angle bracket (>).

```
console>
```

The default host name is "Console" unless it has been changed using the `hostname` command in the Global Configuration mode.

**Privileged EXEC Mode**

Privileged access is password protected to prevent unauthorized use because many of the privileged commands set operating system parameters. The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the Privileged EXEC mode. To enter the Privileged EXEC mode from the User EXEC mode, perform the following steps:

1. At the prompt enter the command `enable` and press <Enter>. A password prompt is displayed.
2. Enter the password and press <Enter>. The password is displayed as "*". The Privileged EXEC mode prompt is displayed. The Privileged EXEC mode prompt consists of the device "host name" followed by "#".

```
console#
```

To return from Privileged Exec mode to User EXEC mode, type the `disable` command at the command prompt.
The following example illustrates how to access Privileged Exec mode and return back to the User EXEC mode:

```
console>enable
Enter Password: ******
console#
console#disable
console>
```

The Exit command is used to return from any mode to the previous mode except when returning to User EXEC mode from the Privileged EXEC mode. For example, the Exit command is used to return from the Interface Configuration mode to the Global Configuration mode.

**Global Configuration Mode**

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface. The Privileged EXEC mode command `configure` is used to enter the Global Configuration mode.

To enter the Global Configuration mode perform the following steps:

1. At the Privileged EXEC mode prompt enter the command `configure` and press `<Enter>`. The Global Configuration mode prompt is displayed. The Global Configuration mode prompt consists of the device "host name" followed by the word "(config)" and "#".

```
console(config)#
```

To return from the Global Configuration mode to the Privileged EXEC mode, the user can use one of the following commands:

- `exit`
- `end`
- `Ctrl+Z`

The following example illustrates how to access Global Configuration mode and returns to the Privileged EXEC mode:

```
console#
console#configure
console(config)#exit
console(config)#exit
```

Using the CLI | 59
### Interface Configuration Mode and Specific Configuration Modes

Interface Configuration mode commands are to modify specific interface operations. The following are the Interface Configuration modes:

- **Line Interface**—Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The Global Configuration mode command `line` is used to enter the Line Configuration command mode.

- **VLAN Database**—Contains commands to create a VLAN as a whole. The Global Configuration mode command `vlan database` is used to enter the VLAN Database Interface Configuration mode.

- **Management Access List**—Contains commands to define management access-lists. The Global Configuration mode command `management access-list` is used to enter the Management Access List Configuration mode.

- **Ethernet**—Contains commands to manage port configuration. The Global Configuration mode command `interface ethernet` is used to enter the Interface Configuration mode to configure an Ethernet type interface.

- **Port Channel**—Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The Global Configuration mode command `interface port-channel` is used to enter the Port Channel Interface Configuration mode.

- **SSH Public Key-chain**—Contains commands to manually specify other device SSH public keys. The Global Configuration mode command `crypto key pubkey-chain ssh` is used to enter the SSH Public Key-chain Configuration mode.

- **Interface**—Contains commands that configure the interface. The Global Configuration mode command `interface ethernet` is used to enter the Interface Configuration mode.

- **QoS**—Contains commands related to service definitions. The Global Configuration mode command `qos config-services` is used to enter the QoS services configuration mode.

### Starting the CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch is managed by entering command keywords and parameters at the prompt. Using the switch command-line interface (CLI) is very similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure the device has an IP address defined, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

**NOTE:** The following steps are for use on the console line only.

To start using the CLI, perform the following steps:
1 Start the device and wait until the startup procedure is complete.
   The User Exec mode is entered, and the prompt "Console>" is displayed.

2 Configure the device and enter the necessary commands to complete the required tasks.

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

When a different user is required to log onto the system, in the Privileged EXEC mode command mode the login command is entered. This effectively logs off the current user and logs on the new user.

**Editing Features**

**Entering Commands**

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 g5," show, interfaces and status are keywords, ethernet is an argument that specifies the interface type, and g5 specifies the port.

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

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

When working with the CLI, the command options are not displayed. The command is not selected from a menu but is manually entered. To see what commands are available in each mode or within an interface configuration, the CLI does provide a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request help is `?`.

There are two instances where the help information can be displayed:

- **Keyword lookup**—The character `?` is entered in place of a command. A list of all valid commands and corresponding help messages are displayed.

- **Partial keyword lookup**—A command is incomplete and the character `?` is entered in place of a parameter. The matched parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Keyboard Shortcuts
Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-arrow key</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl+P</td>
<td></td>
</tr>
<tr>
<td>Down-arrow key</td>
<td>Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.</td>
</tr>
</tbody>
</table>

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see history.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see history size.

To display the history buffer, see show history.

Negating the Effect of Commands

For many configuration commands, the prefix keyword "no" can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

If the command entered is incomplete, invalid, or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing the <Tab> button, an incomplete command is entered. If the characters already entered are not enough for the system to identify a single matching command, press '?' to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicates that the command interface ethernet requires a missing parameter.

```
(config)#interface ethernet
%missing mandatory parameter
(config)#interface ethernet
```
Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

<table>
<thead>
<tr>
<th>Keyboard Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-arrow key</td>
<td>Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Down-arrow key</td>
<td>Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.</td>
</tr>
<tr>
<td>Ctrl+A</td>
<td>Moves the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl+E</td>
<td>Moves the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl+Z/End</td>
<td>Returns back to the Privileged EXEC mode from any mode.</td>
</tr>
<tr>
<td>Backspace key</td>
<td>Moves the cursor back one space.</td>
</tr>
</tbody>
</table>

CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>In a command line, square brackets indicates an optional entry.</td>
</tr>
<tr>
<td>{ }</td>
<td>In a command line, curly brackets indicate a selection of compulsory parameters separated by the</td>
</tr>
<tr>
<td>Italic font</td>
<td>Indicates a parameter.</td>
</tr>
<tr>
<td>&lt;Enter&gt;</td>
<td>Any individual key on the keyboard. For example click &lt;Enter&gt;.</td>
</tr>
<tr>
<td>Ctrl+F4</td>
<td>Any combination keys pressed simultaneously on the keyboard.</td>
</tr>
<tr>
<td>Screen Display</td>
<td>Indicates system messages and prompts appearing on the console.</td>
</tr>
<tr>
<td>all</td>
<td>When a parameter is required to define a range of ports or parameters and all is an option, the default for the command is all when no parameters are defined. For example, the command <code>interface range port-channel</code> has the option of either entering a range of channels, or selecting all. When the command is entered without a parameter, it automatically defaults to all.</td>
</tr>
</tbody>
</table>
AAA Commands

aaa authentication login

The aaa authentication login Global Configuration mode commands defines login authentication. To return to the default configuration, use the no form of this command.

Syntax
aaa authentication login {default | list-name} method1 [method2...]
no aaa authentication login {default | list-name}

- default—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- list-name—Character string used to name the list of authentication methods activated when a user logs in.
- method1 [method2... ]—Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS servers for authentication.</td>
</tr>
</tbody>
</table>

Default Configuration
The local user database is checked. This has the same effect as the command aaa authentication login list-name local.

NOTE: On the console, login succeeds without any authentication check if the authentication method is not defined.

Command Mode
Global Configuration mode

User Guidelines
- The default and optional list names created with the aaa authentication login command are used with the login authentication command.
• Create a list by entering the `aaa authentication login list-name method` command for a particular protocol, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.
• The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

**Example**
The following example configures authentication login.

```console
Console (config)# aaa authentication login default radius local enable none
```

**aaa authentication enable**
The `aaa authentication enable` Global Configuration mode command defines authentication method lists for accessing higher privilege levels. To return to the default configuration use the `no` form of this command.

**Syntax**
```console
aaa authentication enable {default | list-name} method1 [method2...]
```
```console
no aaa authentication enable default
```
• `default`—Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
• `list-name`—Character string used to name the list of authentication methods activated, when using access higher privilege levels.
• `method1 [method2... ]`—Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication. Uses username &quot;$enabx$.&quot; where x is the privilege level.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication. Uses username &quot;$enabx$.&quot; where x is the privilege level.</td>
</tr>
</tbody>
</table>
Default Configuration

If the default list is not set, only the enable password is checked. This has the same effect as the command `aaa authentication enable default enable`.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command `aaa authentication enable default enable none`.

Command Mode

Global Configuration mode

User Guidelines

- The default and optional list names created with the `aaa authentication enable` command are used with the `enable authentication` command.
- Create a list by entering the `aaa authentication enable list-name method` command where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.
- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.
- All `aaa authentication enable default` requests sent by the device to a RADIUS or TACACS server include the username "$enabl35$".

Example

The following example sets authentication when accessing higher privilege levels.

```
Console (config)# aaa authentication enable default enable
```

login authentication

The `login authentication` Line Configuration mode command specifies the login authentication method list for a remote telnet, SSH or console. To return to the default specified by the authentication login command, use the `no` form of this command.

Syntax

```
login authentication {default | list-name}
no login authentication
```

- `default`—Uses the default list created with the `authentication login` command.
- `list-name`—Uses the indicated list created with the `authentication login` command.
AAA Commands

Default Configuration
Uses the default set with the command authentication login.

Command Mode
Line Configuration mode

User Guidelines
- Changing login authentication from default to another value may disconnect the telnet session.

Example
The following example specifies the default authentication method for a console.

```
Console (config)# line console
Console (config-line)# login authentication default
```

enable authentication

The enable authentication Line Configuration mode command specifies the authentication method list when accessing a higher privilege level from a remote telnet, SSH or console. To return to the default specified by the enable authentication command, use the no form of this command.

Syntax
```
enable authentication {default | list-name}
no enable authentication
```

- default—Uses the default list created with the authentication enable command.
- list-name—Uses the indicated list created with the authentication enable command.

Default Configuration
Uses the default set with the command authentication enable.

Command Mode
Line Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example specifies the default authentication method when accessing a higher privilege level from a console.
ip http authentication

The `ip http authentication` Global Configuration mode command specifies authentication methods for http. To return to the default, use the `no` form of this command.

**Syntax**

```
ip http authentication method1 [method2...]
no ip http authentication
```

- `method1 [method2...]`—Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Configuration**

The local user database is checked. This has the same effect as the command `ip http authentication local`.

**Command Mode**

Global Configuration mode

**User Guidelines**

- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

**Example**

The following example configures the http authentication.

```
Console (config)# line console
Console (config-line)# enable authentication default
```

```
Console (config)# ip http authentication radius local
Console (config)# ip http authentication tacacs local
```
ip https authentication

The **ip https authentication** Global Configuration mode command specifies authentication methods for https servers. To return to the default, use the **no** form of this command.

**Syntax**

```
ip https authentication method1 [method2...]
oip https authentication
```

- **method1 [method2...]**—Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Configuration**

The local user database is checked. This has the same effect as the command **ip https authentication local**.

**Command Mode**

Global Configuration mode

**User Guidelines**

- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

**Example**

The following example configures https authentication.

```
Console (config)# ip https authentication radius local
Console (config)# ip https authentication tacacs local
```

**show authentication methods**

The **authentication methods** Privilege EXEC mode command displays information about the authentication methods.
Syntax
  show authentication methods

Default Configuration
  This command has no default configuration.

Command Mode
  Privileged EXEC mode

User Guidelines
  • There are no user guidelines for this command.

Example
  The following example displays the authentication configuration.
The **password** Line Configuration mode command specifies a password on a line. To remove the password, use the **no** form of this command.

**Syntax**

```
password password [encrypted]
```

```
no password
```

- **password**—Password for this level, from 1 to 159 characters in length.
- **encrypted**—Encrypted password to be entered, copied from another device configuration.
**Default Configuration**

No password is required.

**Command Mode**

Line Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example specifies a password "secret" on a line.

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

**enable password**

The `enable password` Global Configuration mode command sets a local password to control access to normal and privilege levels. To remove the password requirement, use the `no` form of this command.

**Syntax**

```
enable password [level level] password [encrypted]
no enable password [level level]
```

- `password`—Password for this level, from 1 to 159 characters in length.
- `level level`—Level for which the password applies. If not specified the level is 15 (Range: 1-15).
- `encrypted`—Encrypted password entered, copied from another device configuration.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.
Example
The following example sets a local level 15 password "secret" to control access to user and privilege levels.

```
Console (config)# enable password level 15 secret
```

username
The `username` Global Configuration mode command establishes a username-based authentication system. To remove a user name use the `no` form of this command.

**Syntax**
```
username name [password password] [level level] [encrypted]

no username name
```
- `name`—The name of the user. (Range: 1 - 20 characters)
- `password`—The authentication password for the user. (Range: 1 - 159 characters).
- `level`—The user level (Range: 1 - 15).
- `encrypted`—Encrypted password entered, copied from another device configuration.

**Default Configuration**
No user is defined.

**Command Mode**
Global Configuration mode

**User Guidelines**
- No password is required.

Example
The following example configures user "bob" with the password "lee" and user level 15 to the system.

```
Console (config)# username bob password lee level 15
```

show users accounts
The `show users accounts` Privileged EXEC mode command displays information about the local user database.
Syntax
  show users accounts

Default Configuration
  This command has no default configuration.

Command Mode
  Privileged EXEC mode

User Guidelines
  • There are no user guidelines for this command.

Example
  The following example displays the local users configured with access to the system.

```
Console# show users accounts

<table>
<thead>
<tr>
<th>Username</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>15</td>
</tr>
<tr>
<td>Robert</td>
<td>15</td>
</tr>
</tbody>
</table>
```
Address Table Commands

bridge address

The bridge address VLAN Interface Configuration mode command adds a static MAC-layer station source address to the bridge table. To delete the MAC address, use the no form of the bridge address command (using the no form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Syntax

bridge address mac-address {ethernet interface | port-channel port-channel-number} [permanent | delete-on-reset | delete-on-timeout | secure]

no bridge address [mac-address]

- interface—A valid Ethernet port.
- port-channel-number—A valid port-channel number.
- permanent—The address can only be deleted by the no bridge address command.
- delete-on-reset—The address is deleted after reset.
- delete-on-timeout—The address is deleted after "age out" time has expired.
- secure—The address is deleted after the port changes mode to unlock learning (no port security command). This parameter is only available when the port is in learning locked mode.

Default Configuration

No static addresses are defined. The default mode for an added address is permanent.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port g8 to the bridge table.
bridge multicast filtering

The bridge multicast filtering Global Configuration mode command enables filtering of multicast addresses. To disable filtering of multicast addresses, use the no form of the bridge multicast filtering command.

Syntax

bridge multicast filtering
no bridge multicast filtering

Default Configuration

Disabled. All multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

- If devices exist on the VLAN, do not change the unregistered multicast addresses state to drop on the devices ports.
- If multicast routers exist on the VLAN and IGMP-snooping is not enabled, the bridge multicast forward-all command should be used to enable forwarding all multicast packets to the multicast routers.

Example

In this example, bridge multicast filtering is enabled.

```
Console (config)# bridge multicast filtering
```

bridge multicast address

The bridge multicast address Interface Configuration mode command registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group. To unregister the MAC address, use the no form of the bridge multicast address command.

Syntax

bridge multicast address {mac-multicast-address | ip-multicast-address}
bridge multicast address {mac-multicast-address | ip-multicast-address} [add | remove] {ethernet interface-list | port-channel port-channel-number-list}

no bridge multicast address {mac-multicast-address | ip-multicast-address}

- add—Adds ports to the group. If no option is specified, this is the default option.
- remove—Removes ports from the group.
- ip-multicast-address—IP multicast address.
- interface-list—Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- port-channel-number-list—Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

Default Configuration
No multicast addresses are defined.

Command Mode
Interface configuration (VLAN) mode

User Guidelines
- If the command is executed without add or remove, the command only registers the group in the bridge database.
- Static multicast addresses can only be defined on static VLANs.

Examples
The following example registers the MAC address:

```
Console (config)# interface vlan 8
Console (config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following example registers the MAC address and adds ports statically.

```
Console (config)# interface vlan 8
Console (config-if)# bridge multicast address 01:00:5e:02:02:03 add ethernet g1-9
```
**bridge multicast forbidden address**

The **bridge multicast forbidden address** Interface Configuration mode command forbids adding a specific multicast address to specific ports. Use the **no** form of this command to return to default.

**Syntax**

```plaintext
bridge multicast forbidden address {mac-multicast-address | ip-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-number-list}

no bridge multicast forbidden address {mac-multicast-address | ip-multicast-address}
```

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ip-multicast-address**—IP multicast address is in the format xxx.xxx.xxx.xxx.
- **interface-list**—Separate non consecutive valid Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- **port-channel-number-list**—Separate non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

**Default Configuration**

No forbidden addresses are defined.

**Command Modes**

Interface Configuration (VLAN) mode

**User Guidelines**

- Before defining forbidden ports, the multicast group should be registered.

**Examples**

In this example the MAC address 01:00:5e:02:02:03 is forbidden on port g9 within VLAN 8.

```
Console (config)# interface vlan 8
Console (config-if)# bridge multicast address 01:00:5e:02:02:03
Console (config-if)# bridge multicast forbidden address 01:00:5e:02:02:03 add ethernet g9
```
bridge multicast forward-all

The bridge multicast forward-all Interface Configuration mode command enables forwarding of all multicast packets on a port. To restore the default, use the no form of the bridge multicast forward-all command.

Syntax

bridge multicast forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}

no bridge multicast forward-all

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **interface-list**—Separate non consecutive valid Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- **port-channel-number-list**—Separate non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

**Default Configuration**

Disable forward-all on the specified interface.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

In this example all multicast packets on port g8 are forwarded.

```
Console (config)# interface vlan 2
Console (config-if)# bridge multicast forward-all add ethernet g8
```

bridge multicast forbidden forward-all

The bridge multicast forbidden forward-all Interface Configuration mode command forbids a port to be a forward-all-multicast port. To restore the default, use the no form of the bridge multicast forward-all command.
Syntax

bridge multicast forbidden forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}

no bridge multicast forward-all

- add—Forbids forwarding all multicast packets.
- remove—Does not forbid forwarding all multicast packets.
- interface-list—Separates non consecutive valid Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- port-channel-number-list—Separates non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

By default, this setting is disabled (for example, forwarding to the port is not forbidden).

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- IGMP snooping dynamically discovers multicast router ports. When a multicast router port is discovered, all the multicast packets are forwarded to it unconditionally.
- This command prevents a port to be a multicast router port.

Example

In this example, forwarding all multicast packets to g6 are forbidden.

```
Console (config)# interface vlan 2
Console (config-if)# bridge multicast forbidden forward-all add ethernet g6
```

bridge aging-time

The `bridge aging-time` Global Configuration mode command sets the address table aging time. To restore the default, use the `no` form of the `bridge aging-time` command.

Syntax

```
bridge aging-time seconds
no bridge aging-time
```
• seconds—Time is number of seconds. (Range: 10 - 630 seconds)

Default Configuration
300 seconds

Command Mode
Global Configuration mode

User Guidelines
• There are no user guidelines for this command.

Example
In this example the bridge aging time is set to 250.

```
Console (config)# bridge aging-time 250
```

clear bridge
The clear bridge Privileged EXEC mode command removes any learned entries from the forwarding database.

Syntax
clear bridge
• This command has no keywords or arguments.

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
• There are no user guidelines for this command.

Example
In this example, the bridge tables are cleared.

```
Console# clear bridge
```
**port security**

The **port security** Interface Configuration mode command locks the port. By locking the port, new addresses are not learned on the port. To enable new address learning, use the **no** form of the **port security** command.

**Syntax**

```
port security [forward | discard | discard-shutdown] [trap seconds]
no port security
```

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

In this example, frame forwarding is enabled without learning, and with traps sent every 100 seconds on port g1.

```
Console (config)# interface ethernet g1
Console (config-if)# port security forward trap 100
Console (config-if)# port security discard trap 100
Console (config-if)# port security discard-shutdown trap 100
```
port security routed secure-address

The `port security routed secure-address` Interface Configuration mode command adds MAC-layer secure addresses to a routed port. Use the `no` form of this command to delete the MAC addresses.

Syntax

```
port security routed secure-address mac-address
no port security routed secure-address mac-address
```


Default Configuration

No addresses are defined.

Command Mode

Interface configuration (Ethernet, port-channel). Cannot be configured for a range of interfaces (range context).

User Guidelines

- The command enables adding secure MAC addresses to a routed ports in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Example

In this example, the MAC-layer address 66:66:66:66:66:66 is added to port g1.

```
Console (config)# interface ethernet g1
```

show bridge address-table

The `show bridge address-table` Privileged EXEC mode command displays all entries in the bridge-forwarding database.

Syntax

```
show bridge address-table [vlan vlan] [ethernet interface | port-channel port-channel-number]
```

- `vlan`—Specific valid VLAN, such as VLAN 1.
- `interface`—A valid Ethernet port.
- `port-channel-number`—A valid port-channel number.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- Internal usage VLANs (VLANs that are automatically allocated on routed ports) would be presented in the VLAN column by a port number and not by a VLAN ID.

**Example**
In this example, all classes of entries in the bridge-forwarding database are displayed.
show bridge address-table static

The show bridge address-table static Privileged EXEC mode command displays statically created entries in the bridge-forwarding database.

Syntax

```
show bridge address-table static [vlan vlan] [ethernet interface | port-channel port-channel-number]
```

- `vlan`—Specific valid VLAN, such as VLAN 1.
- `interface`—A valid Ethernet port.
- `port-channel-number`—A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

In this example, all static entries in the bridge-forwarding database are displayed.
show bridge address-table count

The `show bridge address-table count` Privileged EXEC mode command displays the number of addresses present in all VLANs or in a specific VLAN.

Syntax

```
show bridge address-table count [vlan vlan]
```

- `vlan` — Specific VLAN.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- This command displays the count for 1 VLAN, for all VLANs or for a specific port.
- No commas are allowed.

Example

In this example, the number of addresses present in the VLANs are displayed.
show bridge multicast address-table

The `show bridge multicast address-table` Privileged EXEC mode command displays multicast MAC address table information.

**Syntax**

`show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address | ip-multicast-address] [format ip | mac]`

- `vlan_vlan-id`—A VLAN ID value.
- `ip-multicast-address`—An IP multicast address.
- `format`—Multicast address format. Can be `ip` or `mac`. If `format` is unspecified, the default is `mac`.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

In this example, multicast MAC address table information is displayed.

```
Console# show bridge address-table count

Capacity: 8192
Free: 8084
Used: 108

Static addresses: 2
Dynamic addresses: 97
Internal addresses: 9
```
### Address Table Commands

**NOTE:** A multicast MAC address maps to multiple IP addresses, as shown above.

#### Console # `show bridge multicast address-table`

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01:00:5e:02:02:03</td>
<td>static</td>
<td>g1, g2</td>
</tr>
<tr>
<td>19</td>
<td>01:00:5e:02:02:08</td>
<td>static</td>
<td>g1-8</td>
</tr>
<tr>
<td>19</td>
<td>01:00:5e:02:02:08</td>
<td>dynamic</td>
<td>g9-11</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01:00:5e:02:02:03</td>
<td>g8</td>
</tr>
<tr>
<td>19</td>
<td>01:00:5e:02:02:08</td>
<td>g8</td>
</tr>
</tbody>
</table>

#### Console # `show bridge multicast address-table format ip`

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224-239.130</td>
<td>2.2.3</td>
<td>static</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130</td>
<td>2.2.8</td>
<td>static</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130</td>
<td>2.2.8</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224-239.130</td>
<td>2.2.3</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130</td>
<td>2.2.8</td>
</tr>
</tbody>
</table>
**show bridge multicast filtering**

The `show bridge multicast filtering` Privileged EXEC mode command displays the multicast filtering configuration.

**Syntax**

```
show bridge multicast filtering vlan-id
```

- *vlan_id*—A valid VLAN ID value.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

In this example, the multicast configuration for VLAN 1 is displayed.

```
Console # show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Static</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>Forbidden</td>
<td>Filter</td>
</tr>
<tr>
<td>g2</td>
<td>Forward</td>
<td>Forward(s)</td>
</tr>
<tr>
<td>g3</td>
<td>-</td>
<td>Forward(d)</td>
</tr>
</tbody>
</table>
```

**show ports security**

The `show ports security` Privileged EXEC mode command displays the port-lock status.

**Syntax**

```
show ports security [ethernet interface | port-channel port-channel-number]
```

- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel number.
Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.

Example
In this example, all classes of entries in the port-lock status are displayed.

```
Console # show ports security

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Action</th>
<th>Trap</th>
<th>Frequency</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>Locked</td>
<td>Discard</td>
<td>Enable</td>
<td>100</td>
<td>88</td>
</tr>
<tr>
<td>g2</td>
<td>Unlocked</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>g3</td>
<td>Locked</td>
<td>Discard,</td>
<td>Disable</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shutdown</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Frequency: Minimum time in seconds between consecutive traps
Counter: Number of actions since last trap
```
Clock

clock set

The clock set Privileged EXEC mode command manually sets the system clock.

Syntax

```
clock set hh:mm:ss day month year
```

or

```
clock set hh:mm:ss month day year
```

- `hh:mm:ss`—Current time in hours (military format), minutes, and seconds (0 - 23, mm: 0 - 59, ss: 0 - 59).
- `day`—Current day (by date) in the month (1 - 31).
- `month`—Current month using the first three letters by name (Jan, ..., Dec).

Default Configuration

The default time set is 0:0:0:0 Jan 1 2000 or xxxxx Month Day Year.

Command Mode

Privileged EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example sets the system time to 13:32:00 on the 7th March 2002.

```
Console# clock set 13:32:00 7 Mar 2002
```

clock source

The clock source Privileged EXEC mode command configures an external time source for the system clock.

Syntax

```
clock source {sntp}
```

- no clock source
- `sntp`—SNTP servers
Default Configuration
No external clock source

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.

Examples
The following example configures an external time source for the system clock.

```
Console# clock source sntp
```

clock timezone
The `clock timezone` Global Configuration mode command sets the time zone for display purposes. To set the time to Coordinated Universal Time (UTC), use the `no` form of this command.

Syntax
```
clock timezone hours-offset [minutes minutes-offset] [zone acronym]
no clock timezone
```

- `hours-offset`—Hours difference from UTC. (Range: -12 – +13)
- `minutes minutes-offset`—Minutes difference from UTC. (Range: 0 – 59)
- `zone acronym`—The acronym of the time zone. (Range: Up to 4 characters)

Default Configuration
UTC

Command Mode
Global Configuration mode

User Guidelines
- The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Examples
The following example sets the timezone to 6 hours difference from UTC.

```
Console# (config)# clock timezone -6 zone CST
```
clock summer-time

The **clock summer-time** Global Configuration mode command configures the system to automatically switch to summer time (daylight saving time). To configure the software to not automatically switch to summer time, use the **no** form of this command.

**Syntax**

- `clock summer-time recurring {usa | eu | {week day month hh:mm week day month hh:mm}}`  
  *[offset offset] [zone acronym]*
- `clock summer-time date date month year hh:mm date month year hh:mm [offset offset] [zone acronym]`
- `clock summer-time date month date year hh:mm month date year hh:mm [offset offset] [zone acronym]`

**no clock summer-time**

- **recurring**—Indicates that summer time should start and end on the corresponding specified days every year.
- **date**—Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa**—The summer time rules are the United States rules.
- **eu**—The summer time rules are the European Union rules.
- **week**—Week of the month. (Range: 1 - 4, first, last)
- **day**—Day of the week (Range: first three letters by name, like sun)
- **date**—Date of the month (Range: 1 - 31)
- **month**—Month (Range: first three letters by name)
- **year**—Year - no abbreviation (Range: 2000 - 2097)
- **hh:mm**—Time in military format, in hours and minutes (Range: hh: 0 - 23, mm:0 - 59)
- **offset offset**—Number of minutes to add during summer time (Range: 1 - 1440).
- **zone acronym**—The acronym of the time zone to be displayed when summer time is in effect. If unspecified default to the timezone acronym. (Range: Up to 4 characters)

**Default Configuration**

Summer time is disabled.

**offset offset**—default is 60

**zone acronym**— If unspecified default to the timezone acronym.

If the timezone has not been defined, the default will be UTC.
Command Mode
Global Configuration mode

User Guidelines
• In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.
• USA rule for daylight saving time:
  • Start: First Sunday in April
  • End: Last Sunday in October
  • Time: 2 am local time
• EU rule for daylight saving time:
  • Start: Last Sunday in March
  • End: Last Sunday in October
  • Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

Examples
The following example sets summer time starting on the first Sunday in April at 2am and finishing on the last Sunday in October at 2 am.

```
Console (config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

sntp authentication-key
The sntp authentication-key Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the no form of this command.

Syntax
```
sntp authentication-key number md5 value
no sntp authentication-key number
```

- number—Key number (Range: 1 - 4294967295)
- value—Key value (Range: Up to 8 characters)

Default Configuration
No authentication key is defined.
Command Mode
Global Configuration mode

User Guidelines
• Multiple keys can be generated.

Examples
The following example defines the authentication key for SNTP.

```console
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

sntp authenticate
The `sntp authenticate` Global Configuration mode command grants authentication for received Network Time Protocol (NTP) traffic from servers. To disable the feature, use the `no` form of this command.

Syntax
```
sntp authenticate
no sntp authenticate
```
This command has no arguments or keywords.

Default Configuration
No authentication

Command Mode
Global Configuration mode

User Guidelines
• The command is relevant for both unicast and broadcast.

Examples
The following example defines the authentication key for SNTP and grants authentication.

```console
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```
sntp trusted-key

The sntp trusted-key Global Configuration mode command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the no form of this command.

**Syntax**

```
sntp trusted-key key-number
no sntp trusted-key key-number
```

- **key-number**—Key number of authentication key to be trusted. (Range: 1 - 4294967295)

**Default Configuration**

Not trusted.

**Command Mode**

Global configuration mode

**User Guidelines**

- The command is relevant for both received unicast and broadcast.
- If there is at least 1 trusted key, then unauthenticated messages will be ignored.

**Examples**

The following example authenticates key 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

sntp client poll timer

The sntp client poll timer Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. To return to default, use the no form of this command.

**Syntax**

```
sntp client poll timer seconds
no sntp client poll timer
```

- **seconds**—Polling interval in seconds (Range: 60-86400)
**Default Configuration**

1024

**Command Mode**

Global configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 120 seconds.

```
Console (config)# sntp client poll timer 120
```

**sntp broadcast client enable**

The `sntp broadcast client enable` Global Configuration mode command enables the Simple Network Time Protocol (SNTP) broadcast clients. To disable the SNTP broadcast clients, use the no form of this command.

**Syntax**

```
sntp broadcast client enable
no sntp broadcast client enable
```

This command has no arguments or keywords.

**Default Configuration**

Disabled

**Command Mode**

Global configuration mode

**User Guidelines**

- The `sntp broadcast client enable` Interface Configuration mode command enables the device to receive broadcast transmissions globally and on ALL interfaces.
- Use the `sntp client enable` Interface Configuration mode command to enable the SNTP client on a specific interface.

**Examples**

The following example enables the SNTP broadcast clients.

```
Console (config)# sntp broadcast client enable
```
**sntp anycast client enable**

The `sntp anycast client enable` Global Configuration mode command enables anycast client. To disable the polling for SNTP broadcast client, use the **no** form of this command.

**Syntax**

```
sntp anycast client enable

no sntp anycast client enable
```

This command has no arguments or keywords.

**Default Configuration**

Disabled

**Command Mode**

Global configuration

**User Guidelines**

- Polling time is determined by the `sntp client poll timer` Global Configuration mode command.
- Use the `sntp client enable` Interface Configuration mode command to enable the SNTP client on a specific interface.

**Examples**

The following example enables anycast clients:

```
Console (config-if)# sntp anycast client enable
```

**sntp client enable (interface)**

The `sntp client enable` Interface Configuration mode command enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive broadcast and unicast updates. To disable the SNTP client, use the **no** form of this command.

**Syntax**

```
sntp client enable

no sntp client enable
```

This command has no arguments or keywords.

**Default Configuration**

Disabled
Command Mode

Interface configuration (Ethernet, Port-Channel, VLAN) mode

User Guidelines

- Use the `sntp client enable` Global Configuration mode command to enable broadcast clients globally.
- Use the `sntp anycast client enable` Global Configuration mode command to enable anycast clients globally.

Examples

The following example enables the SNTP client on the interface.

```
Console (config)# sntp client enable
```

`sntp unicast client enable`

The `sntp unicast client enable` Global Configuration mode command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from servers. To disable requesting and accepting Network Time Protocol (NTP) traffic from servers, use the `no` form of this command.

Syntax

```
sntp unicast client enable
no sntp unicast client enable
```

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

- Use the `sntp server` command to define SNTP servers.

Examples

The following example enables the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from servers.

```
Console (config)# sntp unicast client enable
```
sntp unicast client poll

The `sntp unicast client poll` Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined unicast clients. To disable the polling for SNTP client, use the `no` form of this command.

**Syntax**
```
sntp unicast client poll
no sntp unicast client poll
```

This command has no arguments or keywords.

**Default Configuration**
- Disabled

**Command Mode**
- Global configuration mode

**User Guidelines**
- Polling time is determined by the `sntp client poll timer` Global Configuration mode command.

**Examples**
The following example enables polling for the Simple Network Time Protocol (SNTP) predefined unicast clients.

```
Console (config)# sntp unicast client poll
```

sntp server

The `sntp server` Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a server. To remove a server from the list of NTP servers, use the `no` form of this command.

**Syntax**
```
sntp server ip-address | hostname [poll] [key keyid]
no sntp server host
```

- `ip-address`—IP address of the server.
- `hostname`—Hostname of the server. (Range: 1 - 158 characters)
- `poll`—Enable polling.
- `key keyid`—Authentication key to use when sending packets to this peer. (Range: 1 – 4294967295)
Default Configuration
No servers are defined.

Command Mode
Global Configuration mode

User Guidelines
- Up to 8 SNTP servers can be defined.
- Use the `sntp unicast client enable` Global Configuration mode command to enable predefined unicast clients globally.
- To enable polling you should also use the `sntp unicast client poll` Global Configuration mode command for global enabling.
- Polling time is determined by the `sntp client poll timer` Global Configuration mode command.
- If multiple servers are added then the updates applied are determined by the following: Unicast Server updates take precedence, followed by Anycast and then Broadcast.

Examples
The following example configures the device to accept Network Time Protocol (NTP) traffic from the server on 192.1.1.1.

```
Console (config)# sntp server 192.1.1.1
```

show clock
The `show clock` User EXEC mode command displays the time and date from the system clock.

Syntax
    show clock [detail]
    - **detail**—Shows timezone and summertime configuration.

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode
User Guidelines

- The symbol that precedes the show clock display indicates the following:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>°</td>
<td>Time is not authoritative.</td>
</tr>
<tr>
<td>(blank)</td>
<td>Time is authoritative.</td>
</tr>
<tr>
<td>.</td>
<td>Time is authoritative, but SNTP is not synchronized.</td>
</tr>
</tbody>
</table>

Example

The following example displays the time and date from the system clock.

```
Console# show clock

15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Device> show clock detail

15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```
**show sntp configuration**

The `show sntp configuration` Privileged EXEC mode command shows the configuration of the Simple Network Time Protocol (SNTP).

**Syntax**

```
show sntp configuration
```

This command has no keywords or arguments.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

```
Console# show sntp configuration
Polling interval: 7200 seconds

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server                   Polling    Encryption Key
```
The `show sntp status` Privileged EXEC mode command shows the status of the Simple Network Time Protocol (SNTP).

**Syntax**

```plaintext
show sntp status
```

- This command has no keywords or arguments.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

There are no user guidelines for this command.

**Examples**

The following example shows the status of the SNTP:

```
Console# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server Preference Status Last response Offset [mSec] Delay [mSec]
------- ------- ------- -------------- ------ -------
176.1.1.8 Primary Up AFE252C1.6DBDFF2 7.33 117.79
```

---

<table>
<thead>
<tr>
<th>Server</th>
<th>Preference</th>
<th>Status</th>
<th>Last response</th>
<th>Offset</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.1.1.8</td>
<td>Primary</td>
<td>Up</td>
<td>AFE252C1.6DBDFF2</td>
<td>7.33</td>
<td>117.79</td>
</tr>
</tbody>
</table>
176.1.8.179 Secondary Unknown AFE21789.643287C9 8.98 189.19

<table>
<thead>
<tr>
<th>Broadcast:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>IP address</td>
</tr>
<tr>
<td>------------</td>
<td>--</td>
</tr>
<tr>
<td>176.1.1.8</td>
<td>Primary</td>
</tr>
<tr>
<td>176.1.8.179</td>
<td>Secondary</td>
</tr>
</tbody>
</table>
Configuration and Image Files

delete startup-config

The delete startup-config Privileged EXEC mode command deletes the startup-config file.

Syntax

```
delete startup-config
```

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

• There are no user guidelines for this command.

Examples

The following example deletes the startup-config file.

```
Console# delete startup-config
```

copy

The copy Privileged EXEC mode command copies files from a source to a destination.

Syntax

```
copy source-url destination-url [SNMP]
```

• `source-url`—The source file location URL or reserved keyword being copied.
• `destination-url`—The destination file URL or reserved keyword.
• `SNMP`—Used only when copying from/to `startup-config`. Specifies that the destination/source file is in SNMP format

The following table displays keywords aliases to URL:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Used only when copying from/to <code>startup-config</code>. Specifies that the destination/source file is in SNMP format</td>
</tr>
</tbody>
</table>
Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- The location of a file system dictates the format of the source or destination URL.
- The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

Understanding Invalid Combinations of Source and Destination
Some invalid combinations of source and destination exist. Specifically, the following cannot be copied:
- If the source file and destination file are the same file.
- xmodem cannot be a destination. Can only be copied to image, boot and null.
- tftp cannot be the source and destination on the same copy.
- Active Image is the image the system currently boots from (see "show bootvar" command) or set to boot next from. Non active image is the spare image location.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>Source or destination URL for Flash memory. It’s the default in case a URL is specified without a prefix</td>
</tr>
<tr>
<td>running-config</td>
<td>Represents the current running configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Represents the startup configuration file.</td>
</tr>
<tr>
<td>backup-config</td>
<td>Represents the backup configuration file.</td>
</tr>
<tr>
<td>image</td>
<td>If source file, represent the active image file. If destination file, represent the non-active image file.</td>
</tr>
<tr>
<td>boot</td>
<td>Boot file.</td>
</tr>
<tr>
<td>tftp:</td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is tftp://host/[directory]/filename. The host can be either IP address or hostname.</td>
</tr>
<tr>
<td>xmodem:</td>
<td>Source for the file from a serial connection that uses the Xmodem protocol.</td>
</tr>
<tr>
<td>null:</td>
<td>Null destination for copies or files. A remote file can be copied to null to determine its size.</td>
</tr>
</tbody>
</table>
Copy Character Descriptions:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).</td>
</tr>
<tr>
<td>.</td>
<td>For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.</td>
</tr>
</tbody>
</table>

Copying image file from a Server to Flash Memory

Use the `copy source-url image` command to copy an image file from a server to Flash memory.

Copying boot file from a Server to Flash Memory

Use the `copy source-url boot` command to copy a boot file from a server to Flash memory.

Copying a Configuration File from a Server to the Running Configuration

Use the `copy source-url running-config` command to load a "configuration file" from a network server to the device "running configuration". The configuration is added to the "running configuration" as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous "running configuration" and the loaded "configuration file", with the loaded "configuration file" having precedence.

Copying a Configuration File from a Server to the Startup Configuration

Use the `copy source-url startup-config` command to copy a "configuration file" from a network server to the device "startup configuration". These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the `copy running-config destination-url` command to copy the current configuration file to a network server using TFTP. Use the copy `startup-config destination-url` command to copy the "startup configuration" file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the copy `running-config startup-config` command to copy the "running configuration" to the "startup configuration".

Backup the Running Configuration or Startup Configuration to the Backup Configuration

Use the copy `running-config file` command to backup the running configuration to a backup configuration file. Use the copy `startup-config file` command to backup the startup configuration a backup configuration file.
Example
The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to non active image file.

```
Console# copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]
Copy took 0:01:11 [hh:mm:ss]
```

```
boot system
```

The `boot system` Privileged EXEC mode command specifies the system image that the device loads at startup.

**Syntax**

```
boot system (image-1 | image-2)
```

- **image-1**—Specifies image 1 as the system startup image.
- **image-2**—Specifies image 2 as the system startup image.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- Use the `show bootvar` command to find out which image is the active image.

**Examples**

The following example loads system image 1 for the next device startup.

```
Console# boot system image-1
```
**show running-config**

The `show running-config` Privileged EXEC mode command displays the contents of the currently running configuration file.

**Syntax**

```
show running-config [sort type]
```

- `sort type` — Specifies the sorting type of the file. Can be one of the following values: `interface`, `feature`.

**Default Configuration**

Sort type defaults to `interface` if unspecified.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- `show running-config` does not show all the port configurations under the port. Although the device is already configured with some default parameters, “show running config” on an empty device is empty.
Examples
The following example displays the contents of the running-config file.

```
Console# show running-config
no spanning-tree
vlan database
vlan 2
exit
interface range ethernet g(1-2)
switchport access vlan 2
exit
interface vlan 2
bridge address 00:00:00:00:00:01 ethernet g1
exit
interface ethernet g1
gvrp enable
exit
gvrp enable
interface ethernet g24
ip address dhcp
exit
ip name-server 10.6.1.36
console#
```

**show startup-config**

The `show startup-config` Privileged EXEC mode command displays the startup configuration file contents.

**Syntax**

```
show startup-config [sort type]
```
• sort type —Specifies the sorting type of the file. Can be one of the following values: interface, feature.

Default Configuration
Sort type defaults to interface if unspecified.

Command Mode
Privileged EXEC mode

User Guidelines
• There are no user guidelines for this command.
Examples

The following example displays the contents of the startup-config file.

```console
Console# show startup-config
no spanning-tree
vlan database
vlan 2
exit
interface range ethernet g(1-2)
switchport access vlan 2
exit
interface vlan 2
bridge address 00:00:00:00:00:01 ethernet g1
exit
interface ethernet g1
gvrp enable
exit
exit
gvrp enable
interface ethernet g24
ip address dhcp
exit
ip name-server 10.6.1.36
console#
```

show backup-config

The show backup-config Privileged EXEC mode command displays the backup configuration file contents.

**Syntax**

```
show backup-config
```
**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

**Examples**

```
Console# show backup-config
software version 1.1

hostname device

interface ethernet g1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000

interface ethernet g2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```
show bootvar

The `show bootvar` Privileged EXEC mode command displays the active system image file that the device loads at startup.

**Syntax**

```plaintext
show bootvar
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example displays the active system image file that the device loads at startup.

```
Console# show bootvar
Images currently available on the FLASH
image-1    active (selected for next boot)
image-2    not active
```
Ethernet Configuration Commands

interface ethernet

The `interface ethernet` Global Configuration mode command enters the interface configuration mode to configure an Ethernet type interface.

**Syntax**

```
interface ethernet interface
```

- `interface`—Valid Ethernet port.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example enables ports g8 for configuration.

```
Console(config)# interface ethernet g8
Console(config-if)#
```

interface range ethernet

The `interface range ethernet` Global Configuration mode command enters the interface configuration mode to configure multiple Ethernet type interfaces.

**Syntax**

```
interface range ethernet (port-range | all)
```

- `port-range`—List of valid ports to add. Separate non consecutive ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- `all`—All Ethernet ports.

**Default Configuration**

This command has no default configuration.
Command Mode
Global Configuration mode

User Guidelines
- Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

Example
The following example shows how ports g18 to g20 and ports g22 to g24 are grouped to receive the same command.

```
Console(config)# interface range ethernet g18 - g20, g22 - g24
Console(config-if)#
```

shutdown
The shutdown Interface Configuration mode command disables interfaces. To restart a disabled interface, use the no form of this command.

Syntax
```
shutdown
no shutdown
```

Default Configuration
The interface is enabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
- There are no user guidelines for this command.

Examples
The following example disables port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# shutdown
```
The following example re-enables port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# no shutdown
```

description

The `description` Interface Configuration mode command adds a description to an interface. To remove the description use the `no` form of this command.

**Syntax**

```
description string
no description
```

- `string`—Comment or a description of the port up to 64 characters.

**Default Configuration**

By default, the interface does not have a description.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example adds a description to the Ethernet g5.

```
Console(config)# interface ethernet g5
Console(config-if)# description RD SW#3
```

speed

The `speed` Interface Configuration mode command configures the speed of a given Ethernet interface when not using auto-negotiation. To restore the default, use the `no` form of this command.

**Syntax**

```
speed {100 | 1000 | 10000}
no speed
```

- 100—Force 100 Mbps operation.
• 1000—Force 1000 Mbps operation.
• 10000—Force 10000 Mbps operation.

**Default Configuration**
Maximum port capability.

**Command Mode**
Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**
• The command "no speed" in port-channel context returns each port in the port-channel to its maximum capability.

**Example**
The following example configures the speed operation of Ethernet g5 to force 100-Mbps operation.

```
Console(config)\# interface ethernet g5
Console(config-if)\# speed 100
```

duplex

The `duplex` Interface Configuration mode command configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. To restore the default, use the **no** form of this command.

**Syntax**
duplex {half | full}

no duplex

• half—Force half-duplex operation
• full—Force full-duplex operation

**Default Configuration**
The interface is set to full duplex.

**Command Mode**
Interface Configuration (Ethernet) mode

**User Guidelines**
• Before attempting to force a particular duplex mode on the port operating at 10/100/1000 Mbps, disable the auto-negotiation on that port.
• Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

Example
The following example configures the duplex operation of Ethernet g5 to force full duplex operation.

```
Console(config)# interface ethernet g5
Console(config-if)# duplex full
```

negotiation

The negotiation Interface Configuration mode command enables auto-negotiation operation for the speed and duplex parameters of a given interface. To disable negotiation, use the no form of this command.

Syntax
```
negotiation
no negotiation
```

Default Configuration
```
auto-negotiation
```

Command Mode
```
Interface Configuration (Ethernet, port-channel) mode
```

User Guidelines
• Turning off auto-negotiation on an aggregate link may, under some circumstances, make it non-operational. If the other side has auto-negotiation turned on, it may re-synchronize all members of the aggregated link to half-duplex operation, and may, as per the standards, set them all inactive.

Example
The following example enables autonegotiation on Ethernet g5.

```
Console(config)# interface ethernet g5
Console(config-if)# negotiation
```

flowcontrol

The flowcontrol Interface Configuration mode command configures the Flow Control on a given interface. To restore the default, use the no form of this command.
Syntax

```
flowcontrol {auto | on | off}

no flowcontrol
```

- **auto**—Enables auto-negotiation of Flow Control.
- **on**—Enables Flow Control.
- **off**—Disables Flow Control.

**Default Configuration**
Flow Control is off.

**Command Mode**
Interace configuration (Ethernet, port-channel) mode

**User Guidelines**
- Flow Control will operate only if duplex mode is set to FULL. Back Pressure will operate only if duplex mode is set to HALF.
- When Flow Control is ON, the head-of-line-blocking mechanism of this port is disabled.
- If a link is set to NOT use auto-negotiation, the other side of the link must also be configured to not use auto-negotiation.
- To select **auto**, ensure negotiation for Flow Control is enabled.

**Example**
In the following example, Flow Control is enabled on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# flowcontrol on
```

**mdix**
The *mdix* Interface Configuration mode command enables automatic crossover on a given interface. To disable automatic crossover, use the **no** form of this command.

**Syntax**

```
mdix {on | auto}

no mdix
```

- **on**—Manual mdix
- **auto**—Auto mdi/mdix

---

124 | Ethernet Configuration Commands
Default Configuration
Automatic crossover is enabled

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
- **Mdix Auto**: All possibilities to connect a PC with cross OR normal cables are supported and are automatically detected.
- **Mdix ON**: It is possible to connect to a PC only with a normal cable and to connect to another switch ONLY with a cross cable.
- If MDIX is set to "no mdix", the device works opposite from the "MDIX On" behavior. With this setting you can only use either an ethernet standard cross-over cable to connect to a PC, or an ethernet standard cable to connect to another switch.

Example
In the following example, automatic crossover is enabled on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# mdix auto
```

back-pressure

The **back-pressure** Interface Configuration mode command enables Back Pressure on a given interface. To disable Back Pressure, use the **no** form of this command.

Syntax
- `back-pressure`
- `no back-pressure`

Default Configuration
Back Pressure is disabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
- Back Pressure will operate only if duplex mode is set to half.
Example
In the following example Back Pressure is enabled on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# back-pressure
```

**port jumbo-frame**

The `port jumbo-frame` Global Configuration mode command enables jumbo frames for the device. The size of the port jumbo frame is 10K. To disable jumbo frames, use the `no` form of this command.

**Syntax**

```
port jumbo-frame
no port jumbo-frame
```

**Default Configuration**

Jumbo Frames are not enabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

- The command would be effective only after reset.

**Example**

In the following example, Jumbo Frames are enabled on the device.

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

**clear counters**

The `clear counters` User EXEC mode command clears statistics on an interface.

**Syntax**

```
clear counters [ethernet interface | port-channel port-channel-number]
```

- `interface`—Valid Ethernet port.
- `port-channel-number`—Valid port-channel trunk index.

**Default Configuration**

This command has no default configuration.
Command Mode
User EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example
In the following example, the counters for interface g1 are cleared.

```
Console# clear counters ethernet g1
```

**set interface active**

The **set interface active** Privileged EXEC mode command reactivates an interface that was suspended by the system.

**Syntax**

```
set interface active {ethernet interface | port-channel port-channel-number}
```

- `interface`—Valid Ethernet port.
- `port-channel-number`—Valid port-channel trunk index.

**Default Configuration**

This command has no default configuration.

Command Mode
Privilege EXEC mode

User Guidelines

- This command is used to activate interfaces that were configured to be active, but were shutdown for some reason.

Example
The following example activates interface g5, which is disabled.

```
Console# set interface active ethernet g5
```

**show interfaces configuration**

The **show interfaces configuration** Privilege EXEC mode command displays the configuration for all configured interfaces.
Syntax

show interfaces configuration [ethernet interface | port-channel port-channel-number]

- interface—Valid Ethernet port.
- port-channel-number—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Modes

Privilege EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the configuration for all configured interfaces:

```
Console# show interfaces configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>Flow Control</th>
<th>Admin State</th>
<th>Back Pressure</th>
<th>Mdix Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>1G</td>
<td>Full</td>
<td>1000</td>
<td>Auto</td>
<td>On</td>
<td>Up</td>
<td>Enable</td>
<td>Auto</td>
</tr>
<tr>
<td>g2</td>
<td>1G</td>
<td>Full</td>
<td>100</td>
<td>Off</td>
<td>Off</td>
<td>Up</td>
<td>Disable</td>
<td>Off</td>
</tr>
<tr>
<td>g3</td>
<td>1G</td>
<td>Full</td>
<td>1000</td>
<td>Off</td>
<td>Off</td>
<td>Up</td>
<td>Disable</td>
<td>On</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ch</th>
<th>Type</th>
<th>Speed</th>
<th>Neg</th>
<th>Flow Control</th>
<th>Back Pressure</th>
<th>Admin State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1000</td>
<td>1000</td>
<td>Off</td>
<td>Off</td>
<td>Disable</td>
<td>Up</td>
</tr>
</tbody>
</table>
```
The displayed port configuration information includes the following:

- **Port**—The port number.
- **Port Type**—The port designated IEEE shorthand identifier. For example, 1000Base-T refers to 1000 Mbps baseband signaling.
- **Duplex**—Displays the port Duplex status.
- **Speed**—Refers to the port speed.
- **Neg**—Describes the Auto-negotiation status.
- **Flow Control**—Displays the Flow Control status.
- **Back Pressure**—Displays the Back Pressure status.
- **MDIX Mode**—Displays the Auto-crossover status.
- **Admin State**—Displays whether the port is enabled or disabled.

**show interfaces status**

The `show interfaces status` User EXEC mode command displays the status for all configured interfaces.

**Syntax**

```
show interfaces status [ethernet interface | port-channel port-channel-number]
```

- `interface`—A valid Ethernet port.
- `port-channel-number`—A valid port-channel trunk index.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privilege EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the status for all configured interfaces.
Console# `show interfaces status`

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>Flow Control</th>
<th>Back Pressure</th>
<th>MDIX Mode</th>
<th>Link Mode</th>
<th>Link State</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>1G Copper</td>
<td>Full</td>
<td>100</td>
<td>Auto</td>
<td>On</td>
<td>Enable</td>
<td>Off</td>
<td>Disable</td>
<td>Down *</td>
</tr>
<tr>
<td>g2</td>
<td>1G Copper</td>
<td>Full</td>
<td>100</td>
<td>Off</td>
<td>Off</td>
<td>Disable</td>
<td>On</td>
<td>Disable</td>
<td>Up</td>
</tr>
<tr>
<td>g23</td>
<td>1G Fiber</td>
<td>Full</td>
<td>1000</td>
<td>Off</td>
<td>Off</td>
<td>Disable</td>
<td>On</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

Ch Type Duplex Speed Neg Flow Control Back Pressure Link Mode Link State

--- ---- ----- --- ----- ------- ------- -----

1 1000 Full 1000 Off Off Disable Up

* The interface was suspended by the system.
The displayed port status information includes the following:

- **Port**—The port number.
- **Description**—If the port has a description, the description is displayed.
- **Port Type**—The port designated IEEE shorthand identifier. For example, 1000Base-T refers to 1000 Mbps baseband signaling.
- **Duplex**—Displays the port Duplex status.
- **Speed**—Refers to the port speed.
- **Neg**—Describes the Auto-negotiation status.
- **Flow Control**—Displays the Flow Control status.
- **Back Pressure**—Displays the Back Pressure status.
- **Link State**—Displays the Link Aggregation status.

### show interfaces description

The **show interfaces description** User EXEC mode command displays the description for all configured interfaces.

**Syntax**

```
show interfaces description [ethernet interface | port-channel port-channel-number]
```

- **interface**—Valid Ethernet port.
- **port-channel-number**—A valid port-channel trunk index.

**Default Configuration**

This command has no default configuration.

**Command Modes**

Privilege EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the description for the interface g1.
The `show interfaces counters` User EXEC mode command displays traffic seen by the physical interface.

**Syntax**

```
show interfaces counters [ethernet interface | port-channel port-channel-number]
```

- **interface**—A valid Ethernet port.
- **port-channel-number**—A valid port-channel index.

**Default Configuration**

This command has no default configuration.

**Command Modes**

Privilege EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example displays traffic seen by the physical interface:

```
show interfaces counters
```

---

```
Port Description
---- ------------------
g1 Management_port

g2 R&D_port

g3 Finance_port

Ch Description
---- ------------------
Ch 1 Output
```
<table>
<thead>
<tr>
<th>Port</th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>183892</td>
<td>1289</td>
<td>987</td>
<td>8</td>
</tr>
<tr>
<td>g2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g3</td>
<td>123899</td>
<td>1788</td>
<td>373</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>g4</td>
<td>9188</td>
<td>9</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>g5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g6</td>
<td>8789</td>
<td>27</td>
<td>8</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ch</th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>27889</td>
<td>928</td>
<td>0</td>
<td>78</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ch</th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>23739</td>
<td>882</td>
<td>0</td>
<td>122</td>
</tr>
</tbody>
</table>
The following example displays counters for port g1.

```
Console# show interfaces counters ethernet g1

<table>
<thead>
<tr>
<th>Port</th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>183892</td>
<td>1289</td>
<td>987</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>9188</td>
<td>9</td>
<td>8</td>
<td>0</td>
</tr>
</tbody>
</table>

FCS Errors: 8
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Internal MAC Tx Errors: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>Counted received octets.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>Counted received unicast packets.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InMcastPkts</td>
<td>Counted received multicast packets.</td>
</tr>
<tr>
<td>InBcastPkts</td>
<td>Counted received broadcast packets.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Counted transmitted octets.</td>
</tr>
<tr>
<td>OutUcastPkts</td>
<td>Counted transmitted unicast packets.</td>
</tr>
<tr>
<td>OutMcastPkts</td>
<td>Counted transmitted multicast packets.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>Counted transmitted broadcast packets.</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>A count of frames received that are not an integral number of octets in length and do not pass the FCS check.</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>Counted frames received that are an integral number of octets in length but do not pass the FCS check.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>Counted frames that are involved in a single collision, and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>A count of frames that are involved in more than one collision and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>SQE Test Errors</td>
<td>A count of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.</td>
</tr>
<tr>
<td>Deferred Transmissions</td>
<td>A count of frames for which the first transmission attempt is delayed because the medium is busy.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>Counted times that a collision is detected later than one slotTime into the transmission of a packet.</td>
</tr>
<tr>
<td>Excessive Collisions</td>
<td>Counted frames for which transmission fails due to excessive collisions.</td>
</tr>
<tr>
<td>Internal MAC Tx Errors</td>
<td>Counted frames for which transmission fails due to an internal MAC sublayer transmit error.</td>
</tr>
<tr>
<td>Carrier Sense Errors</td>
<td>The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.</td>
</tr>
<tr>
<td>Oversize Packets</td>
<td>Counted frames received that exceed the maximum permitted frame size.</td>
</tr>
<tr>
<td>Internal MAC Rx Errors</td>
<td>Counted frames for which reception fails due to an internal MAC sublayer receive error.</td>
</tr>
</tbody>
</table>
**show ports jumbo-frame**

The `show ports jumbo-frame` User EXEC mode command displays the jumbo frames configuration.

**Syntax**

```plaintext
show ports jumbo-frame
```

**Default Configuration**

This command has no default configuration.

**Command Modes**

User EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

| 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. 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. 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. For an interface operating at 10 Gb/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 `Receive Error` on the XGMII. |
| Received Pause Frames | Counted MAC Control frames received with an opcode indicating the PAUSE operation. |
| Transmitted Pause Frames | Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. |
Example
The following example displays the jumbo frames configuration.

```
Console# show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

**port storm-control include-multicast**

The `port storm-control include-multicast` Global Configuration mode command enables the device to count multicast packets together with broadcast packets. To disable counting of multicast packets, use the `no` form of this command.

**Syntax**
```
port storm-control include-multicast
no port storm-control include-multicast
```

There are no arguments or keywords for this command.

**Default Configuration**
Multicast packets are not counted.

**Command Modes**
Global Configuration mode

**User Guidelines**
- To control multicasts storms use the commands `port storm-control broadcast enable` and `port storm-control broadcast rate`.

Example
The following example enables the counting of multicast packets.

```
Console# configure
Console(config)# port storm-control include-multicast
```

**port storm-control broadcast enable**

The `port storm-control broadcast enable` Interface Configuration mode command enables broadcast storm control. To disable broadcast storm control, use the `no` form of this command.

**Syntax**
```
port storm-control broadcast enable
```
no port storm-control broadcast enable

**Default Configuration**
Broadcast storm control is disabled.

**Command Modes**
Interface Configuration (Ethernet) mode

**User Guidelines**
- Use the `port storm-control broadcast rate` Interface Configuration mode command to set the maximum allowable broadcast rate.
- Multicast can be counted as part of the "storm" frames if the `port storm-control include-multicast` Global Configuration mode command is already executed.

**Example**
The following example enables broadcast storm control on port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# port storm-control broadcast enable
```

**port storm-control broadcast rate**
The `port storm-control broadcast rate` Interface Configuration mode command configures the maximum broadcast rate. Use the `no` form of this command to return to the default value.

```
port storm-control broadcast rate rate
no port storm-control broadcast rate
```

- `rate`—Maximum kilobytes per second of broadcast and multicast traffic on a port. (Rate: 0-65535)

**Default Configuration**
The default storm control broadcast rate is 1000.

**Command Mode**
Global Configuration mode

**User Guidelines**
- Use the `port storm-control broadcast enable` Interface Configuration mode command to enable broadcast storm control.
- The granularity is 1 - 64K packets. Note that if the rate is 0, broadcast packets are not forwarded.
Example
The following example configures the maximum broadcast rate 10 kilobytes per second.

```
console(config)# interface ethernet g2
console(config-if)# port storm-control broadcast rate 10
```

**show ports storm-control**

The `show ports storm-control` Privileged EXEC mode command displays the storm control configuration.

**Syntax**

```
show ports storm-control [interface]
```

- `interface`—A valid Ethernet port.

**Default Configuration**

This command has no default configuration.

**Command Modes**

- Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the storm control configuration.

```
console(config)# port storm-control broadcast rate 333
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Broadcast Storm control [Packets/sec]</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>333</td>
</tr>
<tr>
<td>g2</td>
<td>Disabled</td>
</tr>
<tr>
<td>g3</td>
<td>333</td>
</tr>
<tr>
<td>g4</td>
<td>Disabled</td>
</tr>
<tr>
<td>g5</td>
<td>Disabled</td>
</tr>
<tr>
<td>g6</td>
<td>Disabled</td>
</tr>
<tr>
<td>g7</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Console# show ports storm-control

---

Ethernet Configuration Commands | 139
| g8  | Disabled |
| g9  | Disabled |
| g10 | Disabled |
| g11 | Disabled |
| g12 | Disabled |
| g13 | Disabled |
| g14 | Disabled |
| g15 | Disabled |
| g16 | Disabled |
| g17 | Disabled |
| g18 | Disabled |
| g19 | Disabled |
| g20 | Disabled |
| g21 | Disabled |
| g22 | Disabled |
| g23 | Disabled |
| g24 | Disabled |
GVRP Commands

gvrp enable (global)

GVRP, or GARP VLAN Registration Protocol, is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single switch is manually configured with all desired VLANs for the network, and all other switches on the network learn these VLANs dynamically.

The `gvrp enable` Global Configuration mode command enables GVRP globally. To disable GVRP globally on the switch, use the `no` form of this command.

Syntax

```
gvrp enable
no gvrp enable
```

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example globally enables GVRP on the device.

```
Console (config)# gvrp enable
```

gvrp enable (interface)

The `gvrp enable` Interface Configuration mode command enables GVRP on an interface. To disable GVRP on an interface, use the `no` form of this command.

Syntax

```
gvrp enable
no gvrp enable
```

Default Configuration

GVRP is disabled on all interfaces by default.
Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- An access port would not dynamically join a VLAN because it is always a member in only one VLAN.
- Membership in an untagged VLAN would be propagated in a same way as a tagged VLAN. i.e. in such a case it’s the administrator’s responsibility to set the PVID to be the untagged VLAN VID.

Example

The following example enables GVRP on ethernet g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp enable
```

garp timer

The `garp timer` Interface Configuration mode command adjusts the GARP application join, leave, and leaveall GARP timer values. To reset the timer to default values, use the `no` form of this command.

Syntax

```
garp timer {join | leave | leaveall} timer_value
```

- **no garp timer**
  - `join`—Indicates the time in milliseconds that PDUs are transmitted. (Range: 10-2147483640)
  - `leave`—Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The Leave Time is activated by a Leave All Time message sent/received, and cancelled by the Join message. (Range: 10-2147483640)
  - `leaveall`—Used to confirm the port within the VLAN. The time in milliseconds between messages sent. (Range: 10-2147483640)

- **timer_value**—Timer values in milliseconds.

Default Configuration

The default timer values are as follows:

- Join timer—200 milliseconds
- Leave timer—600 milliseconds
- Leaveall timer—10000 milliseconds
**Command Mode**

Interface configuration (Ethernet, port-channel) mode

**User Guidelines**

- The `timer_value` value must be a multiple of 10.
- You must maintain the following relationship for the various timer values:
  - Leave time must be greater than or equal to three times the join time.
  - Leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP application will not operate successfully.

**Example**

The following example sets the leave timer for port g8 to 900 milliseconds.

```
Console (config)# interface ethernet g8
Console (config-if)# garp timer leave 900
```

**gvrp vlan-creation-forbid**

The `gvrp vlan-creation-forbid` Interface Configuration mode command enables or disables dynamic VLAN creation. To disable dynamic VLAN creation, use the `no` form of this command.

**Syntax**

```
gvrp vlan-creation-forbid
no gvrp vlan-creation-forbid
```

**Default Configuration**

By default, dynamic VLAN creation is enabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.
Example
The following example disables dynamic VLAN creation on port g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp vlan-creation-forbid
```

gvrp registration-forbid

The `gvrp registration-forbid` Interface Configuration mode command de-registers all dynamic VLANs, and prevents dynamic VLAN registration on the port. To allow dynamic registering for VLANs on a port, use the `no` form of this command.

Syntax
```
gvrp registration-forbid
no gvrp registration-forbid
```

Default Configuration
Dynamic registering and deregistering for each VLAN on the port is allowed.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp registration-forbid
```

clear gvrp statistics

The `clear gvrp statistics` Privileged EXEC mode command clears all the GVRP statistics information.

Syntax
```
clear gvrp statistics [ethernet interface | port-channel port-channel-number]
```
- `interface`—A valid Ethernet interface.
- `port-channel-number`—A valid port-channel trunk index.
Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example clears all the GVRP statistics information on port g8.

```
Console# clear gvrp statistics ethernet g8
```

show gvrp configuration

The show gvrp configuration User EXEC mode command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

Syntax
```
show gvrp configuration [ethernet interface | port-channel port-channel-number]
```

• `interface`—A valid Ethernet interface.
• `port-channel-number`—A valid port-channel trunk index.

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example shows how to display GVRP configuration information:
show gvrp statistics

The `show gvrp statistics` User EXEC mode command displays GVRP statistics.

**Syntax**

```
show gvrp statistics [ethernet interface | port-channel port-channel-number]
```

- `interface`—A valid Ethernet interface.
- `port-channel-number`—A valid trunk index.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode

**User Guidelines**

- There are no user guidelines for this command.
Example
The following example shows GVRP statistics information:

```console
Console# show gvrp statistics

GVRP statistics:
----------------
  rJE : Join Empty Received  rJIn : Join In Received
  rEmp : Empty Received      rLIn : Leave In Received
  rLE  : Leave Empty Received rLA  : Leave All Received
  sJE  : Join Empty Sent     sJIn : Join In Sent
  sEmp : Empty Sent          sLIn : Leave In Sent
  sLE  : Leave Empty Sent    sLA  : Leave All Sent

| Port | rJE | rJIn | rEmp | rLIn | rLE | rLA | sJE | sJIn | sEmp | sLIn | sLE | sLA |
|------|-----|------|------|------|-----|-----|-----|-----|------|------|-----|-----|-----|
| g1   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g2   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g3   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g4   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g5   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g6   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g7   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
| g8   | 0   | 0    | 0    | 0    | 0   | 0   | 0   | 0   | 0    | 0    | 0   | 0   |
```

**show gvrp error-statistics**

The `show gvrp error-statistics` User EXEC mode command displays GVRP error statistics.
Syntax

show gvrp error-statistics [ethernet interface | port-channel port-channel-number]

  - interface—port.
  - port-channel-number—A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example displays GVRP statistics information.

```
Console# show gvrp-error statistics

GVRP error statistics:
----------------------
Legend:
INVPROT : Invalid Protocol Id  INVPLEN : Invalid PDU Length
INVATYP : Invalid Attribute Type  INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value  INVEVENT : Invalid Event

<table>
<thead>
<tr>
<th>Port</th>
<th>INVPROT</th>
<th>INVATYP</th>
<th>INVAVAL</th>
<th>INVALEN</th>
<th>INVEVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>g8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
IGMP Snooping Commands

ip igmp snooping (Global)

The `ip igmp snooping` Global Configuration mode command enables Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping use the `no` form of this command.

**Syntax**

```
  ip igmp snooping
  no ip igmp snooping
```

**Default Configuration**

IGMP snooping is disabled.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example enables IGMP snooping.

```
Console (config)# ip igmp snooping
```

ip igmp snooping (Interface)

The `ip igmp snooping` Interface Configuration mode command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the `no` form of this command.

**Syntax**

```
  ip igmp snooping
  no ip igmp snooping
```

**Default Configuration**

IGMP snooping is disabled on all VLANs in the set context.

**Command Mode**

Interface configuration (VLAN) mode
User Guidelines

- IGMP snooping can only be enabled on static VLANs.

Example

The following example enables IGMP snooping on VLAN 2.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping
```

ip igmp snooping mrouter

The `ip igmp snooping mrouter` Interface Configuration mode command enables automatic learning of multicast router ports in the context of a specific VLAN. To remove automatic learning of multicast router ports, use the `no` form of this command.

Syntax

```
ip igmp snooping mrouter learn-pim-dvmrp
no ip igmp snooping mrouter learn-pim-dvmrp
```

Default Configuration

Automatic learning of mrouter ports is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- Multicast router ports can be configured statically by the `bridge multicast forward-all` command.

Example

The following example enables automatic learning of multicast router ports on VLANs.

```
Console (config) # interface vlan 2
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

ip igmp snooping host-time-out

The `ip igmp snooping host-time-out` Interface Configuration mode command configures the host-time-out. If an IGMP report for a multicast group was not received for a host-time-out period, from a specific port, this port is deleted from the member list of that multicast group. To reset to default host-time-out use the `no` form of this command.
Syntax
   ip igmp snooping host-time-out time-out
   no ip igmp snooping host-time-out
   •  time-out—Host timeout in seconds. (Range: 1 - 2147483647)

Default Configuration
   The default host-time-out is 260 seconds.

Command Mode
   Interface Configuration (VLAN) mode

User Guidelines
   •  The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

Example
   The following example configures the host timeout to 300 seconds.
   
   Console (config)# interface vlan 2
   Console (config-if)# ip igmp snooping host-time-out 300

ip igmp snooping mrouter-time-out

The ip igmp snooping mrouter-time-out Interface Configuration mode command configures the mrouter-time-out. The mrouter-time-out command is used for setting the aging-out time after multicast router ports are automatically learned. To configure the default mrouter-time-out, use the no form of this command.

Syntax
   ip igmp snooping mrouter-time-out time-out
   no ip igmp snooping mrouter-time-out
   •  time-out—mrouter timeout in seconds (Range: 1 - 2147483647)

Default Configuration
   The default value is 300 seconds.

Command Mode
   Interface Configuration (VLAN) mode
User Guidelines

- There are no user guidelines for this command.

Example

The following example configures the mrouter timeout to 200 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping mrouter-time-out 200
```

**ip igmp snooping leave-time-out**

The `ip igmp snooping leave-time-out` VLAN Interface Configuration mode command configures the leave-time-out. If an IGMP report for a multicast group is not received within the leave-time-out period after an IGMP leave was received from a specific port, the current port is deleted from the member list of that multicast group. To configure the default leave-time-out, use the `no` form of this command.

**Syntax**

```
ip igmp snooping leave-time-out {time-out | immediate-leave}

no ip igmp snooping leave-time-out
```

- `time-out`—leave-time-out in seconds. (Range: 0 - 2147483647)
- `immediate-leave`—Specifies that the port should be immediately removed from the members list after receiving IGMP Leave.

**Default Configuration**

The default leave-time-out configuration is 10 seconds.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

- The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP Query.
- Use `immediate leave` only where there is only one host connected to a port.

**Example**

The following example configures the host leave-time-out to 60 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping leave-time-out 60
```
**show ip igmp snooping mrouter**

The `show ip igmp snooping mrouter` User EXEC mode command displays information on dynamically learned multicast router interfaces.

**Syntax**

show ip igmp snooping mrouter [interface vlan-id]

- `vlan_id`—VLAN ID value.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example shows IGMP snooping mrouter information.

```
Console # show ip igmp snooping mrouter

VLAN     Ports
-------- ------
2         g1
```

**show ip igmp snooping interface**

The `show ip igmp snooping interface` User EXEC mode command displays IGMP snooping configuration.

**Syntax**

show ip igmp snooping interface `vlan-id`

- `vlan_id`—VLAN ID value.

**Default Configuration**

This command has no default configuration.
IGMP Snooping Commands

Command Mode
User EXEC mode

User Guidelines
- There are no user guidelines for this command.

Example
The example displays IGMP snooping information.

```
Console # show ip igmp snooping interface 1
IGMP Snooping is globally disabled
IGMP Snooping is disabled on VLAN 1
IGMP host timeout is 260 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 60 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

```
show ip igmp snooping groups
```

The `show ip igmp snooping groups` User EXEC mode command displays the multicast groups learned by IGMP snooping.

Syntax
```
show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address]
```
- `vlan_id`—VLAN ID value.
- `ip-multicast-address`—IP multicast address.

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
- To see the full multicast address table (including static addresses) use the `show bridge address-table` command.
**Example**

The example shows IGMP snooping information.

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Querier</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224-239.130</td>
<td>Yes</td>
<td>g1, g2</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130</td>
<td>Yes</td>
<td>g9-11</td>
</tr>
</tbody>
</table>
IP Addressing Commands

clear host dhcp

The `clear host dhcp` Privileged EXEC mode command deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

Syntax

```
clear host dhcp {name | *}
```

- **name**: Particular host entry to remove. (Range: 1 - 158 characters.)
- *****: Removes all entries.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- This command would delete the host name-to-address mapping temporarily until the next renew of the IP address.

Examples

The following example deletes all entries from the host name-to-address mapping.

```
Console# clear host dhcp *
```

ip address

The `ip address` Interface Configuration mode command sets an IP address. To remove an IP address, use the `no` form of this command.

Syntax

```
ip address ip-address {mask | prefix-length}
no ip address [ip-address]
```

- **ip-address**: IP address
- **mask**: Specifies the network mask of the IP address. (Range: Valid Subnet mask)
prefix-length—The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8 - 30)

Default Configuration
No IP address is defined for interfaces.

Command Mode
Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines
• An IP address cannot be configured for a range of interfaces (range context).

Example
The following example configures VLAN 1 with the IP address 131.108.1.27 and subnet mask 255.255.255.0.

```console
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

**ip address dhcp**

The `ip address dhcp` Interface Configuration mode command acquires an IP address on an interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure any acquired address, use the `no` form of this command.

The `no ip address dhcp` command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

**Syntax**

```
ip address dhcp [hostname host-name]
```

```
o ip address dhcp
```

• `hostname`—Specifies the host name. (Range: 1 - 20 characters)

• `host-name`—DHCP host name. This name need not be the same as the host name entered in global configuration mode.

Default Configuration
This command has no default configuration.

Command Mode
Interface configuration (Ethernet, VLAN, port-channel)
User Guidelines

- The `ip address dhcp` command allows any interface to dynamically learn its IP address by using the DHCP protocol.
- Some DHCP Servers require that the DHCPDISCOVER message have a specific host name. The most typical usage of the `ip address dhcp hostname host-name` command is when `host-name` is the host name provided by the system administrator.
- If a device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.
- If the `ip address dhcp` command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the device globally configured host name.
- However, you can use the `ip address dhcp hostname host-name` command to place a different name in the DHCP option 12 field than the globally configured host name of the device.
- The `no ip address dhcp` command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

Example

The following example acquires an IP address on an Ethernet interface from DHCP.

```plaintext
Console (config)# interface ethernet g8
Console (config-if)# ip address dhcp
```

**ip default-gateway**

The `ip default-gateway` Global Configuration mode command defines a default gateway (router). To remove the default gateway use the `no` form of this command.

**Syntax**

```
ip default-gateway ip-address

no ip default-gateway
```

- `ip-address` — Valid IP address that specifies the IP address of the default gateway.

**Default Configuration**

No default gateway is defined.

**Command Mode**

Global configuration
User Guidelines

- There are no User Guidelines for this command.

Example

The following example defines an ip default gateway.

```
Console(config)# ip default-gateway 192.168.1.1
```

show ip interface

The `show ip interface` User EXEC mode command displays the usability status of interfaces configured for IP.

Syntax

```
show ip interface [ethernet interface-number | vlan vlan-id | port-channel number]
```

- `ethernet interface-number`—port.
- `vlan vlan-id`—VLAN number.
- `port-channel number`—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example the displays the usability status of interfaces configured for IP.
arp

The `arp` Global Configuration mode command adds a permanent entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the `no` form of this command.

**Syntax**
```
arp ip_addr hw_addr {ethernet interface-number | vlan vlan-id | port-channel number}
no arp ip_addr {ethernet interface-number | vlan vlan-id | port-channel number}
```

- `ip_addr`—IP address or IP alias to map to the specified MAC address.
- `hw_addr`—MAC address to map to the specified IP address or IP alias.
- `ethernet interface-number`—Ethernet port number.
- `vlan vlan-id`—VLAN number.
- `port-channel number`—Port-channel number.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
- The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not need to be specified.
Example
The following example adds the IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console (config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet g8
```

arp timeout

The `arp timeout` Global Configuration mode command configures how long an entry remains in the ARP cache. To restore the default value, use the `no` form of this command.

**Syntax**
```
arp timeout seconds
no arp timeout
```
- *seconds*—Time (in seconds) that an entry remains in the ARP cache. (Range: 1 - 40000000)

**Default Configuration**
The default timeout is 60000 seconds.

**Command Mode**
Global Configuration mode

**User Guidelines**
- It is recommended not to set the timeout value to less than 3600.

**Example**
The following example configures ARP timeout to 12000 seconds.

```
Console (config)# arp timeout 12000
```

clear arp-cache

The `clear arp-cache` Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

**Syntax**
```
clear arp-cache
```

**Default Configuration**
This command has no default configuration.
Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

show arp

The show arp Privileged EXEC mode command displays entries in the ARP table.

Syntax
   show arp

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example displays entries in the ARP table.

```
Console# show arp
ARP timeout: 60000 Seconds

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>HW address</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>10.7.1.102</td>
<td>00:10:B5:04:DB:4B</td>
<td>Dynamic</td>
</tr>
<tr>
<td>g2</td>
<td>10.7.1.135</td>
<td>00:50:22:00:2A:A4</td>
<td>Static</td>
</tr>
</tbody>
</table>
```
**ip domain-lookup**

The `ip domain-lookup` Global Configuration mode command enables the IP Domain Naming System (DNS)-based host name-to-address translation. To disable the DNS, use the `no` form of this command.

**Syntax**

```plaintext
ip domain-lookup
no ip domain-lookup
```

This command has no arguments or keywords.

**Default Configuration**

Enabled

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example enables the IP Domain Naming System (DNS)-based host name-to-address translation.

```
Console (config)# ip domain-lookup
```
Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.

Examples
The following example defines a default domain name of www.dell.com.

console (config)# ip domain-name www.dell.com

ip name-server

The `ip name-server` Global Configuration mode command sets the available name servers. To remove a name server, use the `no` form of this command.

Syntax
```
ip name-server server-address [server-address2 ... server-address8]
no ip name-server [server-address1 ... server-address8]
```
- `server-address`—IP addresses of the name server. Up to 8 servers can be defined in one command or by using multiple commands.

Default Configuration
No name server addresses are specified.

Command Mode
Global Configuration mode

User Guidelines
- The preference of the servers is determined by the order they were entered.
- Up to 8 servers can be defined.

Examples
The following example sets the available name server.

console (config)# ip name-server 176.16.1.18

ip host

The `ip host` Global Configuration mode command defines a static host name-to-address mapping in the host cache. To remove the name-to-address mapping, use the `no` form of this command.
Syntax

```
ipo host name address

no ip host name
```

- `name`—Name of the host (Range: 1 - 158 characters)
- `address`—Associated IP address.

**Default Configuration**

No host is defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example defines a static host name-to-address mapping in the host cache.

```
Console (config)# ip host accounting.dell.com 176.10.23.1
```

**clear host**

The `clear host` Privileged EXEC mode command deletes entries from the host name-to-address cache.

**Syntax**

```
clear host {name | *}
```

- `name`—Particular host entry to remove. (Range: 1 - 158 characters)
- `*`—Removes all entries.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.
Examples
The following example deletes entries from the host name-to-address cache.

```console
Console (config)# clear host *
```

show hosts
The show hosts User EXEC mode command displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.

Syntax
- `show hosts [name]`
  - `name`—Name of the host.(Range: 1 - 158 characters)

Default Configuration

Command Mode
- User EXEC mode

User Guidelines
- There are no user guidelines for this command.

Examples
The following example displays host information.
show hosts
Default domain is GM.COM
Name/address lookup is enabled
Name servers: 176.16.1.18 176.16.1.19
Static host name-to-address mapping:

<table>
<thead>
<tr>
<th>Host</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.dell.com">www.dell.com</a></td>
<td>176.16.8.8 176.16.8.9</td>
</tr>
</tbody>
</table>

Cache:

<table>
<thead>
<tr>
<th>Host</th>
<th>TTL(Hours)</th>
<th>Total</th>
<th>Elapsed</th>
<th>Type</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.dell.com">www.dell.com</a></td>
<td>72</td>
<td>3</td>
<td>IP</td>
<td>171.64.14.203</td>
<td></td>
</tr>
</tbody>
</table>
**LACP Commands**

**lACP system-priority**

The `lACP system-priority` Global Configuration mode command configures the system priority. To reset to default, use the `no` form of this command.

**Syntax**

```
  lACP system-priority value
```

```
  no lACP system-priority
```

- `value`—Value of the priority. (Range: 1 - 65535)

**Default Configuration**

The default system priority value is 1.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example configures the system priority to 120.

```
Console (config)# lACP system-priority 120
```

**lACP port-priority**

The `lACP port-priority` Interface Configuration mode command configures the priority value for physical ports. To reset to default priority value, use the `no` form of this command.

**Syntax**

```
  lACP port-priority value
```

```
  no lACP port-priority
```

- `value`—Port priority value. (Range: 1 - 65535)

**Default Configuration**

The default port priority value is 1.
Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example configures the priority value for port g8 to 247.

```
Console (config)# interface ethernet g8
Console (config-if)# lacp port-priority 247
```

**lacp timeout**

The `lacp timeout` Interface Configuration mode command assigns an administrative LACP timeout. To reset the default administrative LACP timeout use the no form of this command.

**Syntax**

```
lacp timeout {long | short}
no lacp timeout
```

- **long**—Specifies a long timeout value.
- **short**—Specifies a short timeout value.

**Default Configuration**

The default port timeout value is long.

**Command Mode**

Interface Configuration (Ethernet) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example assigns an administrative LACP timeout for port g8 to a long timeout value.

```
Console (config)# interface ethernet g8
Console (config-if)# lacp timeout long
```
**show lacp ethernet**

The `show lacp ethernet` Privilege EXEC mode command displays LACP information for Ethernet ports.

**Syntax**

```
show lacp ethernet [interface | parameters | statistics | protocol-state]
```

- `Interface`—Ethernet interface.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privilege EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example shows how to display LACP statistics information.

```
Console# show lacp ethernet g1 statistics
Port g1 LACP Statistics:
LACP PDUs sent:2

LACP PDUs received:2
```

**show lacp port-channel**

The `show lacp port-channel` Privileged EXEC mode command displays LACP information for a port-channel.

**Syntax**

```
show lacp port-channel [port_channel_number]
```

- `port_channel_number`—The port-channel number.

**Default Configuration**

This command has no default configuration.
Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example shows how to display LACP port-channel information.

```
Console# show lACP port-channel 1
Port-Channel 1:Port Type 1000 Ethernet
   Actor
       System Priority:1
       MAC Address: 00:02:85:0E:1C:00
       Admin Key:    29
       Oper Key:     29

   Partner
       System Priority:0
       MAC Address: 00:00:00:00:00:00
       Oper Key:     14
```
Line Commands

line
The `line` Global Configuration mode command identifies a specific line for configuration and enters the line configuration command mode.

**Syntax**

```
line {console | telnet | ssh}
```

- `console`—Console terminal line.
- `telnet`—Virtual terminal for remote console access (Telnet).
- `ssh`—Virtual terminal for secured remote console access (SSH).

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example configures the device as a virtual terminal for remote console access.

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

speed

The `speed` Line Configuration mode command sets the line baud rate.

**Syntax**

```
speed bps
```

- `bps`—Baud rate in bits per second (bps). The options are 2400, 9600, 19200 and 38400.

**Default Configuration**

This default speed is 9600.
**Command Mode**

Line Configuration (console) mode

**User Guidelines**

- The configured speed would be applied when Autobaud is disabled.
- If Autobaud is disabled, the new speed is implemented immediately.

**Examples**

The following example sets the baud rate to 9600.

```console
Console (config)# line console
Console(config-line)# speed 9600
```

**autobaud**

The `autobaud` Line Configuration mode command sets the line for automatic baud rate detection (autobaud). Use the `no` form of this command to disable automatic baud rate detection.

**Syntax**

`autobaud`

`no autobaud`

**Default Configuration**

Disabled

**Command Mode**

Line Configuration (console) mode

**User Guidelines**

- To start communications using automatic baud detection, press the Enter key twice.

**Examples**

The following example sets the line for automatic baud rate detection.

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

**exec-timeout**

The `exec-timeout` Line Configuration mode command sets the interval that the system waits until user input is detected. To restore the default setting, use the `no` form of this command.
Syntax

```
exec-timeout minutes [seconds]
```

no exec-timeout

- minutes—Integer that specifies the number of minutes. (Range: 0 - 65535)
- seconds—Additional time intervals in seconds. (Range: 0 - 59)

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

- To specify no timeout, enter the `exec-timeout ("0 0")` command.

Examples

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
Console (config)# line console
Console(config-line)# exec-timeout 20
```

show line

The `show line` User EXEC mode command displays line parameters.

Syntax

```
show line [console | telnet | ssh]
```

- console—Console terminal line.
- telnet—Virtual terminal for remote console access (Telnet).
- ssh—Virtual terminal for secured remote console access (SSH).

Default Configuration

Default value is console.

Command Mode

User EXEC mode

User Guidelines

- There are no user guidelines for this command.
Examples
The following example displays the line configuration.

```
console# show line console
Interactive timeout: 10 minutes
History: 10
```

terminal history
The `terminal history` EXEC mode command enables the command history function for the current terminal session. To disable the command history function, use the `no` form of this command.

Syntax
- `terminal history`
- `terminal no history`

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
The command enables the command history for the current session. The default would be determined by the history line configuration command.

terminal history size
The `terminal history size` EXEC mode command changes the command history buffer size for the current terminal session. To reset the command history buffer size to the default, use the `no` form of this command.

Syntax
- `terminal history size number-of-commands`
- `terminal no history size`

- `number-of-commands` - Number of commands the system records in the history buffer (Range: 1-0216).
Default Configuration
  The default is determined by the history size line configuration command.

Command Mode
  User EXEC mode

User Guidelines
  The maximum for the sum of all buffers is 256.
LLDP Commands

lldp enable (global)

To enable Link Layer Discovery Protocol (LLDP), use the lldp enable command in global configuration mode. To disable LLDP, use the no form of this command.

Syntax

lldp enable
no lldp enable

Default Configuration

The command is enabled.

Command Mode

Global configuration

User Guidelines

- There are no guidelines for this command.

Example

The following example enables Link Layer Discovery Protocol (LLDP).

```
console (config)# lldp enable
```

lldp enable (interface)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the lldp enable command in interface configuration mode. To disable LLDP on an interface, use the no form of this command.

Syntax

lldp enable [rx | tx | both]
no lldp enable

- **rx** — Receive only LLDP packets.
- **tx** — Transmit only LLDP packets.
- **both** — Receive and transmit LLDP packets (default)

Default Configuration

Enabled in both modes.
Command Modes
Interface configuration (Ethernet)

User Guidelines
- LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG. LLDP data received through LAG ports is stored individually per port.
- LLDP operation on a port is not dependent on STP state of a port. I.e. LLDP frames are sent and received on blocked ports. If a port is controlled by 802.1X, LLDP operates only if the port is authorized.

Examples
The following example enables Link Layer Discovery Protocol (LLDP) on an interface (g5).

```
Console(config)# interface ethernet g5
Console(config-if)# lldp enable
```

lldp timer

To specify how often the software sends Link Layer Discovery Protocol (LLDP) updates, use the `lldp timer` command in global configuration mode. To revert to the default setting, use the `no` form of this command.

Syntax
```
lldp timer seconds
no lldp timer
```

- `seconds` — Specifies in seconds how often the software sends LLDP update. (Range: 5 - 32768 seconds).

Default Configuration
Default - 30 seconds.

Command Modes
Global configuration

User Guidelines
- There are no user guidelines for this command.
Examples
The following example specifies how often the software sends Link Layer Discovery Protocol (LLDP) updates.

```
Console (config) # lldp timer
```

**lldp hold-multiplier**

To specify the amount of time the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet before discarding it, use the `lldp hold-multiplier` command in global configuration mode. To revert to the default setting, use the `no` form of this command.

**Syntax**

```
lldp hold-multiplier number
no lldp hold-multiplier
```

- `number` — Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value (Range: 2-10).

**Default Configuration**

The default configuration is 4.

**Command Modes**

Global configuration

**User Guidelines**

- The actual time-to-live value used in LLDP frames can be expressed by the following formula: \( \text{TTL} = \min(65535, \text{LLDP-Timer} \times \text{LLDP-HoldMultiplier}) \). For example, if the value of LLDP timer is '30', and the value of the LLDP hold multiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header.

**Examples**

The following example specifies how often the software sends Link Layer Discovery Protocol (LLDP) updates.

```
Console (config) # lldp hold-multiplier 6
```

**lldp reinit-delay**

To specify the minimum time an LLDP port will wait before reinitializing LLDP transmission, use the `lldp reinit-delay` command in global configuration mode. To revert to the default setting, use the `no` form of this command.
Syntax
   lldp reinit-delay seconds
   no lldp reinit-delay
   
   seconds — Specifies the minimum time in seconds an LLDP port will wait before
   reinitializing LLDP transmission. (Range 1-10 seconds).

Default Configuration
   2 seconds

Command Modes
   Global configuration

User Guidelines
   There are no user guidelines for this command.

Examples
   The following example specifies the minimum time an LLDP port will wait before reinitializing
   LLDP transmission.

   Console (config) # lldp reinit-delay 6

lldp tx-delay

To specify the delay between successive LLDP frame transmissions initiated by value/status
changes in the LLDP local systems MIB, use the lldp tx-delay command in global configuration
mode. To revert to the default setting, use the no form of this command.

Syntax
   lldp tx-delay seconds
   no lldp tx-delay

Parameters
   
   seconds — Specifies the delay in seconds between successive LLDP frame transmissions
   initiated by value/status changes in the LLDP local systems MIB. Range 1-8192 second.

Default Configuration
   The default value is 2 seconds

Command Modes
   Global configuration
Usage Guidelines

- It is recommended that the TxDelay would be less than 0.25 of the LLDP timer interval.

Examples

The following example specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.

```
Console (config) # lldp tx-delay 7
```

lldp optional-tlv

To specify which optional TLVs from the basic set should be transmitted, use the lldp optional-tlv command in interface configuration mode. To revert to the default setting, use the no form of this command.

Syntax

```
lldp optional-tlv tlv1 [tlv2 ... tlv5]
```

```
no lldp optional-tlv
```

- **tlv** — Specifies TLV that should be included. Available optional TLVs are: port-desc, sys-name, sys-desc and sys-cap. (Range 1-8192 seconds).

Default Configuration

No optional TLV is transmitted.

Command Modes

Interface configuration (Ethernet)

User Guidelines

- There are no user guidelines for this command.

Example

The following example specifies which optional TLV (2)s from the basic set should be transmitted.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp optional-tlv sys-name
```

lldp management-address

To specify the management address that would be advertised from an interface, use the lldp management-address command in interface configuration mode. To stop advertising management address information, use the no form of this command.
Syntax

lldp management-address ip-address
  no management-address ip
  • ip-address — Specifies the management address to advertise.

Default Configuration

No IP address is advertised.

Command Modes

Interface configuration (Ethernet)

User Guidelines

• Each port can advertise one IP address.
• Only static IP addresses can be advertised.

Example

The following example specifies management address that would be advertised from an interface.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp management-address 192.168.0.1
```

clear lldp rx

To restart the LLDP RX state machine and clearing the neighbors table, use the `clear lldp rx` command in privileged EXEC mode.

Syntax

```
clear lldp rx [ethernet interface]
  • Interface — Ethernet port
```

Command Modes

Privileged EXEC

User Guidelines

• There are no user guidelines for this command.

Example

The following example restarts the LLDP RX state machine and clearing the neighbors table.

```
console (config)#clear lldp rx
```
**show lldp configuration**

To display the Link Layer Discovery Protocol (LLDP) configuration, use the `show lldp configuration` command in privileged EXEC mode.

**Syntax**

```
show lldp configuration [ethernet interface]
```

- `Interface` — Ethernet port

**Command Modes**

Privileged EXEC

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the Link Layer Discovery Protocol (LLDP) configuration

```
Switch# show lldp configuration

Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Optional TLVs</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>RX, TX</td>
<td>PD, SN, SD, SC</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>g2</td>
<td>TX</td>
<td>PD, SN</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>g3</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**show lldp local**

To display the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port, use the `show lldp local` command in privileged EXEC mode.

**Syntax**

```
show lldp local ethernet interface
```

- `Interface` — Ethernet port
Command Modes

Privileged EXEC

User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.

```
Switch# show lldp neighbors ethernet g1
Device ID: 0060.704C.73FF
Port ID: 1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
```

**show lldp neighbors**

To display information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP), use the `show lldp neighbors` command in privileged EXEC mode.

**Syntax**

```
show lldp neighbors [ethernet interface]
```

- **Interface** — Ethernet port

**Command Modes**

Privileged EXEC

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP).
Switch# `show lldp neighbors`

<table>
<thead>
<tr>
<th>Port</th>
<th>Device ID</th>
<th>Port ID</th>
<th>Hold Time</th>
<th>Capabilities</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>0060.704C.73FE</td>
<td>1</td>
<td>117</td>
<td>B</td>
<td>ts-7800-2</td>
</tr>
<tr>
<td>g1</td>
<td>0060.704C.73FD</td>
<td>1</td>
<td>93</td>
<td>B</td>
<td>ts-7800-2</td>
</tr>
<tr>
<td>g2</td>
<td>0060.704C.73FC</td>
<td>9</td>
<td>1</td>
<td>B, R</td>
<td>ts-7900-1</td>
</tr>
<tr>
<td>g3</td>
<td>0060.704C.73FB</td>
<td>1</td>
<td>92</td>
<td>W</td>
<td>ts-7900-2</td>
</tr>
</tbody>
</table>

Switch# `show lldp neighbors ethernet g1`

Device ID: 0060.704C.73FE
Port ID: 1
Hold Time: 117
Capabilities: B
System Name: ts-7800-2
System description:
Port description:
Management address: 172.16.1.1
Management ACL

management access-list

The management access-list Global Configuration mode command defines an access-list for management, and enters the access-list for configuration. Once in the access-list configuration mode, the denied or permitted access conditions are configured with the deny and permit commands. To remove an access list, use the no form of this command.

Syntax

management access-list name

no management access-list name

• name—The access list name using up to 32 characters.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

• This command enters the access-list configuration mode, where the denied or permitted access conditions with the deny and permit commands must be defined.
• If no match criteria are defined the default is "deny".
• If reentering to an access-list context, the new rules are entered at the end of the access-list.
• Use the management access-class command to select the active access-list.
• The active management list cannot be updated or removed.
• Management ACL requires a valid management interface (valid IFindex). A valid management interface is an interface with an IP address. A valid (IFindex) management interface can be a single port, vlan or port-channel. Management ACL only restricts access to the device for management configuration or viewing.
Examples
The following example shows how to create an access-list called "mlist", configure two management interfaces ethernet g1 and ethernet g9, and make the access-list the active list.

```
Console (config)# management access-list mlist
Console (config-macl)# permit ethernet g1
Console (config-macl)# permit ethernet g9
Console (config-macl)# exit
Console (config)# management access-class mlist
```

The following example shows how to create an access-list called "mlist", configure all interfaces to be management interfaces except interfaces ethernet g1 and ethernet g9, and make the access-list the active list.

```
Console (config)# management access-list mlist
Console (config-macl)# deny ethernet g1
Console (config-macl)# deny ethernet g9
Console (config-macl)# permit
Console (config-macl)# exit
Console (config)# management access-class mlist
```

`permit (management)`

The `permit` Management Access-List Configuration mode command defines a permit rule.

**Syntax**

```
permit [ethernet interface-number | vlan vlan-id | port-channel number] [service service]
permit ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service]
```

- **ethernet interface-number**—A valid Ethernet port number.
- **vlan vlan-id**—A valid VLAN number.
- **port-channel number**—A valid port channel number.
- **ip-address**—Source IP address. (Range: Valid IP Address)
- **mask mask**—Specifies the network mask of the source IP address. (Range: Valid subnet mask)
• **mask prefix-length**—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0 - 32)

• **service service**—Indicates service type. Can be one of the following: telnet, ssh, http, https or snmp.

**Default Configuration**

If no `permit` statement is present, the default is set to `deny`.

**Command Mode**

Management Access-list Configuration mode

**User Guidelines**

• Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface. The system supports up to 256 management access rules.

**Example**

The following example shows how all ports are permitted in the access-list called "mlist".

```
Console (config)# management access-list mlist
Console (config-macl)# permit
```

deny (management)

The `deny` Management Access-List Configuration mode command defines a deny rule.

**Syntax**

```bash
deny [ethernet interface-number | vlan vlan-id | port-channel number] [service service]
deny ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service]
```

• **ethernet interface-number**—A valid Ethernet port number.

• **vlan vlan-id**—A valid VLAN number.

• **port-channel number**—A valid port-channel number.

• **ip-address**—Source IP address. (Range: Valid IP Address)

• **mask mask**—Specifies the network mask of the source IP address. (Range: Valid subnet mask)

• **mask prefix-length**—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0 - 32)
• service service—Indicates service type. Can be one of the following: telnet, ssh, http, https or snmp.

Default Configuration
This command has no default configuration.

Command Mode
Management Access-list Configuration mode

User Guidelines
• Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface. The system supports up to 256 management access rules.

Example
The following example shows how all ports are denied in the access-list called "mlist".

```
Console (config)# management access-list mlist
Console (config-macl)# deny
```

management access-class

The management access-class Global Configuration mode command defines which management access-list is used. To disable restriction, use the no form of this command.

Syntax
```
management access-class {console-only | name}
no management access-class
```

name—Name of the access list. If unspecified, defaults to an empty access-list. (Range: 1 - 32 characters)

console-only—The device can be managed only from the console.

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
• There are no user guidelines for this command.
Example
The following example configures an access-list called "mlist" as the management access-list.

```console
Console (config)# management access-class mlist
```

**show management access-list**

The `show management access-list` Privileged EXEC mode command displays management access-lists.

**Syntax**

```
show management access-list [name]
```

- `name`—Name of the access list. If unspecified, defaults to an empty access-list.(Range: 1 - 32 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the active management access-list.

```console
Console# show management access-list
mlist
-----
permit ethernet g1
permit ethernet g9
!
(Note: all other access implicitly denied)
```

**show management access-class**

The `show management access-class` Privileged EXEC mode command displays the active management access-list.
Syntax
show management access-class

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example displays the management access-list information.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```
PHY Diagnostics Commands

test copper-port tdr

The test copper-port tdr Privileged EXEC mode command diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.

Syntax
   test copper-port tdr interface
   •  interface—A valid Ethernet port.

Default Configuration
   This command has no default configuration.

Command Mode
   Privileged EXEC mode

User Guidelines
   •  The port under test should be conducted when the fiber link is down.

   NOTE: The maximum distance VCT can function is 120 meters.

Examples
   The following example results in a report on the cable attached to port g3.

   Console# test copper-port tdr g3
   Cable is open at 100 meters

show copper-ports tdr

The show copper-ports tdr Privileged EXEC mode command display the last TDR (Time Domain Reflectometry) tests on specified ports.

Syntax
   show copper-ports tdr [interface]
   •  interface—A valid Ethernet port.

Default Configuration
   This command has no default configuration.
Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example displays the last TDR (Time Domain Reflectometry) tests on all ports.

```
Console# show copper-ports tdr

<table>
<thead>
<tr>
<th>Port</th>
<th>Result</th>
<th>Length [meters]</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g2</td>
<td>Short</td>
<td>50</td>
<td>13:32:00 23 July 2003</td>
</tr>
<tr>
<td>g3</td>
<td>Test has not been performed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g4</td>
<td>Short</td>
<td>128</td>
<td>13:32:00 23 July 2003</td>
</tr>
<tr>
<td>g5</td>
<td>Fiber</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
```

show copper-ports cable-length
The `show copper-ports cable-length` Privileged EXEC mode command displays the estimated copper cable length attached to a port.

Syntax
- `show copper-ports cable-length [interface]`
  - `interface`—A valid Ethernet port.

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- The port must be active and working in 1000M.
Example
The following example displays the estimated copper cable length attached to all ports.

```
Console# show copper-ports cable-length

<table>
<thead>
<tr>
<th>Port</th>
<th>Length [meters]</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>&lt; 50</td>
</tr>
<tr>
<td>g2</td>
<td>Giga link not active</td>
</tr>
<tr>
<td>g3</td>
<td>110-140</td>
</tr>
</tbody>
</table>
```

show fiber-ports optical-transceiver
The show fiber-ports optical-transceiver Privileged EXEC mode command displays the optical transceiver diagnostics.

Syntax
```
show fiber-ports optical-transceiver [interface] [detailed]
```
- interface—A valid Ethernet port.
- detailed—Detailed diagnostics.

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- To test optical transceivers, ensure a fiber link is up. The test is only supported on Dell supported SFP modules.
Examples
The following example displays the optical transceiver diagnostics.

```
console# show fiber-ports optical-transceiver

+-----------+-----------------+----------+----------+----------+----------+----------+----+
| Port      | Temp            | Voltage  | Current  | Output   | Input    | LOS      |
|-----------|-----------------|----------|----------|----------|----------|----------|----|
|           |                 |          |          | Power    | Power    |          |    |
|           |                 |          | Power    | Power    |          |          |    |
|           |                 |          | Power    | Power    |          |          |    |
|           |                 |          | Power    | Power    |          |          |    |
| g3        | Copper          |          |          |          |          |          |    |
| g21       | W               | OK       | E        | OK       | OK       | OK       |    |
| g22       | OK              | OK       | OK       | OK       | OK       | OK       |    |
```

Temp – Internally measured transceiver temperature.
Voltage – Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX received power.
LOS – Loss of signal
The following example displays detailed optical transceiver diagnostics.

```console
show fiber-ports optical-transceiver detailed
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output Power</th>
<th>Input Power</th>
<th>LOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>g23</td>
<td>70</td>
<td>7.27</td>
<td>0.79</td>
<td>3.30</td>
<td>2.50</td>
<td>No</td>
</tr>
<tr>
<td>g21</td>
<td>70</td>
<td>7.24</td>
<td>0.78</td>
<td>2.20</td>
<td>2.49</td>
<td>No</td>
</tr>
</tbody>
</table>

- **Temp** - Internally measured transceiver temperature.
- **Voltage** - Internally measured supply voltage.
- **Current** - Measured TX bias current.
- **Output Power** - Measured TX output power.
- **Input Power** - Measured RX received power.
- **LOS** - Loss of signal
Port Channel Commands

interface port-channel

The interface port-channel Global Configuration mode command enters the interface configuration mode of a specific port-channel.

Syntax

```
interface port-channel port-channel-number
```

- `port-channel-number`—A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- Eight aggregated links can be defined with up to 8 member ports per port channel. Turning off auto-negotiation of an aggregate link may, under some circumstances, make it non-operational. If the other side has auto-negotiation turned on, it may re-synchronize all members of the aggregated link to half-duplex operation, and may, as per the standards, set them all to inactive.

Example

The following example enters the context of port-channel number 1.

```
Console (config)# interface port-channel 1
```

interface range port-channel

The interface range port-channel Global Configuration mode command enters the interface configuration mode to configure multiple port-channels.

Syntax

```
interface range port-channel {port-channel-range | all}
```

- `port-channel-range`—List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- `all`—All the channel-ports.
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
- Commands under the interface range context are executed independently on each interface in the range: If the command returns an error on one of the interfaces, it will not stop the execution of the command on other interfaces.

Example
The following example shows how port-channels 1, 2 and 8 are grouped to receive the same command.

```
Console (config)# interface range port-channel 1-2
Console (config-if)#
```

channel-group

The `channel-group` Interface Configuration mode command associates a port with a port-channel. To remove a port from a port channel, use the `no` form of this command.

Syntax
```
channel-group port-channel-number mode {on | auto}

no channel-group
```

- `port-channel-number`—Specifies the number of the valid port-channel for the current port to join.
- `on`—Forces the port to join a channel.
- `auto`—Allows the port to join a channel as a result of an LACP operation.

Default Configuration
The port is not assigned to any port-channel.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
- There are no user guidelines for this command.
Example
The following example shows how port g5 is configured to port-channel number 1 without LACP.

```
Console (config)# interface ethernet g5
Console (config-if)# channel-group 1 mode on
```

**port channel load balance**

Use the `port-channel load-balance` global configuration command to configure the load balancing policy of the port channeling. Use the `no` form of this command to reset to default.

**Syntax**
```
port-channel load-balance  {layer-2 | layer-2-3 | layer-2-3-4}
no port-channel load-balance
```

- **layer-2** — Port channel load balancing is based on layer 2 parameters.
- **layer-2-3** — Port channel load balancing is based on layer 2 and layer 3 parameters.
- **layer-2-3-4** — Port channel load balancing is based on layer 2, layer 3 and layer 4 parameters.

**Default Configuration**
Layer 2

**Command Modes**
Global Configuration

**User Guidelines**
- In L2+L3+L4 load balancing policy, fragmented packets might be reordered.

**Example**
The following example configures the load balancing policy of the port channeling on layer 2.

```
Console (config) # port-channel load-balance layer-2
```

**show interfaces port-channel**

Use the `show interfaces port-channel` global configuration command to show Port channel information.

**Syntax**
```
show interfaces port-channel [port-channel-number]
```
• `port_channel_number` — Number of the Port channel to display. (Range: Valid port channel)

**Default Configuration**
This command has no default configuration.

**Command Modes**
EXEC

**User Guidelines**
• There are no user guidelines for this command.

**Example**
The following example shows how all port channel information is displayed.

```
Console# show interfaces port-channel

Load balancing: Layer2 and Layer 3.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active: 1, 2</td>
</tr>
<tr>
<td>2</td>
<td>Active: 2, 7</td>
</tr>
<tr>
<td>3</td>
<td>Active: 3, 8</td>
</tr>
</tbody>
</table>
```
Port Monitor Commands

port monitor

The `port monitor` Interface Configuration mode command starts a port monitoring session. To stop a port monitoring session, use the `no` form of this command.

Syntax

```
port monitor src-interface [rx | tx]
no port monitor src-interface
```

- `src-interface`—Valid Ethernet port or port-channel number.
- `rx`—Monitors received packets only. If no option specified, monitors both rx and tx.
- `tx`—Monitors transmitted packets only. If no option specified, monitors both rx and tx.

Default Configuration

The default is both rx and tx.

Command Mode

Interface Configuration mode

User Guidelines

- This command enables traffic on one port to be copied to another port, or between the source port (src-interface) and a destination port (the port being configured). Only a single target port can be defined per system.
- The port being monitored cannot be set faster than the monitoring port.
- The following restrictions apply to ports configured to be destination ports:
  - The port cannot be already configured as a source port.
  - The port cannot be a member in a port-channel.
  - An IP interface is not configured on the port.
  - GVRP is not enabled on the port.
  - The port is not a member in any VLAN, except for the default VLAN (will automatically be removed from the default VLAN).
- The following restrictions apply to ports configured to be source ports:
  - Port monitoring Source Ports must be simple ports, and not port-channels.
  - The port cannot be already configured as a destination port.
  - All the frames are transmitted as either always tagged or always untagged.
General Restrictions:

- Ports cannot be configured as a group using the `interface range ethernet` command.

**NOTE:** The Port Mirroring target must be a member of the Ingress VLAN of all Mirroring source ports. Therefore, multicast and broadcast frames in these VLANs are seen more than once. (Actually $N$, where $N$ is the number of mirroring source ports).

When both transmit (Tx) and receive (Rx) directions of more than one port are monitored, the capacity may exceed the bandwidth of the target port. In this case, the division of the monitored packets may not be equal. The user is advised to use caution in assigning port monitoring.

**Example**
The following example shows how traffic on port g8 (source port) is copied to port g1 (destination port).

```
Console(config)# interface ethernet g1
Console(config-if)# port monitor g8
```

**show ports monitor**
The `show ports monitor` User EXEC mode command displays the port monitoring status.

**Syntax**
```
show ports monitor
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
User EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example shows how the port copy status is displayed.
## Port Monitor Commands

**Console# show ports monitor**

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>g8</td>
<td>RX, TX</td>
<td>Active</td>
</tr>
<tr>
<td>g2</td>
<td>g8</td>
<td>RX, TX</td>
<td>Active</td>
</tr>
<tr>
<td>g18</td>
<td>g8</td>
<td>Rx</td>
<td>Active</td>
</tr>
</tbody>
</table>
QoS Commands

qos
The qos Global Configuration mode command enables quality of service (QoS) on the device and enters QoS basic mode. Use the no form of this command to disable the QoS features on the device.

Syntax
qos
no qos

Default Configuration
There is no default configuration for this command.

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example shows how QoS is enabled on the device, in basic mode.

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

show qos
The show qos User EXEC mode command displays the quality of service (QoS) mode for the entire device.

Syntax
show qos

This command has no arguments or keywords.

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode
User Guidelines
- There are no user guidelines for this command.

Example
The following example displays a QoS mode.

```
Console# show qos
Trust: dscp

Console# show qos
Qos: disabled
Trust: dscp
```

wrr-queue cos-map
The wrr-queue cos-map Global Configuration mode command maps assigned CoS values to select one of the egress queues. To return to the default values, use the no form of this command.

Syntax
```
wrr-queue cos-map queue-id cos1...cos8
no wrr-queue cos-map [queue-id]
```

- `queue-id`—The queue number to which the following CoS values are mapped.
- `cos1...cos8`—Map to specific queues up to eight CoS values from 0 to 7.

Default Configuration
The map default values for 4 queues:
- CoS value 1 select queue 1
- CoS value 2 select queue 1
- CoS value 0 select queue 2
- CoS value 3 select queue 2
- CoS value 4 select queue 3
- CoS value 5 select queue 3
- CoS value 6 select queue 4
- CoS value 7 select queue 4

Command Mode
Global Configuration mode
User Guidelines

- You can use this command to distribute traffic into different queues, where each queue is configured with different weighted round robin (WRR) parameters.
- To enable the expedite queues, use the `priority-queue out` Interface Configuration mode command `wrr-queue cos-map`.

Example

The following example maps CoS 3 to queue 4.

```
Console (config)# wrr-queue cos-map 4 3
```

wrr-queue bandwidth

The `wrr-queue bandwidth` Interface Configuration mode command assigns Weighted Round Robin (WRR) weights to egress queues. The weights ratio determines the frequency in which the packet scheduler dequeues packets from each queue. To return to the default values, use the `no` form of this command.

Syntax

```
wrr-queue bandwidth weight1 weight2 ... weight_4
no wrr-queue bandwidth
```

- `weight1...weight_4`—Sets the bandwidth ratio by the WRR packet scheduler for the packet queues. Separate each value by spaces. (Range: 6 - 255)

Default Configuration

The default WRR weight is 1/4 ratio for all queues (each weight set to 6).

Command Mode

Interface Configuration (Ethernet, port channel) mode

User Guidelines

- The ratio for each queue is defined by the queue weight divided by the sum of all queue weights (i.e., the normalized weight). This actually sets the bandwidth allocation of each queue.
- A weight of 0 means no bandwidth is allocated for the same queue, and the share bandwidth is divided among the remaining queues.
- All 4 queues are participating excluding the queues that are assigned as expedite queues. The weights of these queues are ignored in the ratio calculation.
- All 4 queues participate in the WRR exclude the expedite queues, in which case the corresponded weight is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.
Example
The following example assigns WRR weights to egress queues.

```
Console(config)# priority-queue num-of-queues 1
Console(config)# interface ethernet g1
Console(config-if)# wrr-queue bandwidth 20 30 50

Console(config)# priority-queue num-of-queues 0
Console(config)# interface ethernet g3
Console(config-if)# wrr-queue bandwidth 20 30 50 10
```

**priority-queue out num-of-queues**
The `priority-queue out num-of-queues` Global Configuration mode command enables the egress queues to be expedite queues. Use the `no` form of this command to return to the default values.

**Syntax**
```
priority-queue out num-of-queues number-of-queues

no priority-queue out num-of-queues
```
- `number-of-queues`—Assign the number of queues to be expedite queues. The expedite queues would be the queues with higher indexes. (Range: 1 - 4)

**Default Configuration**
All queues are expedite queues.

**Command Mode**
Global Configuration mode

**User Guidelines**
- When configuring the `priority-queue out num-of-queues` command, the weighted round robin (WRR) weight ratios are affected because there are fewer queues participating in WRR.
- Queue 4 is taken as the highest index queue. Queue 3 is taken as the next highest queue. If two priority queues are selected then queue 4 and 3 will be used. Leaving queue 2 and 1 for WRR.
Example
The following example sets queue 4, 3 to be expedite queues.

```
Console (config)# priority-queue out num-of-queues 2
```

**show qos interface**
The `show qos interface` User EXEC mode command displays interface QoS data.

**Syntax**
```
show qos interface [ethernet interface-number | queuing]
```
- **ethernet interface-number**—Ethernet port number.
- **queuing**—Displays the queue strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
User EXEC mode

**User Guidelines**
If no keyword is specified with the `show qos interface` command, the port QoS mode (DSCP trusted, CoS trusted, untrusted), default CoS value, attached to the port, attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

**Examples**
The following example displays output from the `show qos interface g1 queuing` command.
The `qos map dscp-queue` Global Configuration mode command modifies the DSCP to queue map. To return to the default map, use the `no` form of this command.

**Syntax**

```
qos map dscp-queue dscp-list to queue-id
```

```
no qos map dscp-queue
```

- `dscp-list`—Specify up to 8 DSCP values, separate each DSCP with a space. (Range: 0 - 63)
- `queue-id`—Enter the queue number to which the DSCP value corresponds.
Default Configuration

The following table describes the default map.

<table>
<thead>
<tr>
<th>DSCP value</th>
<th>0-15</th>
<th>16-31</th>
<th>32-47</th>
<th>48-63</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue-ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration mode

User Guidelines

- Queue settings for 3, 11, 19, ... cannot be modified.

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

qos trust (Global)

The `qos trust` Global Configuration mode command can be used to configure the system to "trust" state. To return to the default state, use the `no` form of this command.

Syntax

```
qos trust {cos | dscp}
```

```
no qos trust
```

- `cos`—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- `dscp`—Classifies ingress packets with the packet DSCP values.

Default Configuration

CoS is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

- Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.
- Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.
- To return to the untrusted state, use the no qos command to apply best effort service.

**Example**
The following example configures the system to DSCP trust state.

```
Console (config)# qos trust dscp
```

**qos trust (Interface)**
The qos trust Interface Configuration mode command enables each port trust state. To disable the trust state on each port, use the no form of this command.

**Syntax**
```
qos trust
no qos trust
```

**Default Configuration**
Each port is enabled while the system is operational.

**Command Mode**
Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**
- Use no qos trust to disable the trust mode on each port.
- Use qos trust to enable trust mode on each port.

**Example**
The following example configures port g5 to default trust state (CoS).

```
Console (config)# interface ethernet g5
Console (config-if)# qos trust
```

**qos cos**
The qos cos Interface Configuration mode command configures the default port CoS value. To return to the default setting, use the no form of this command.

**Syntax**
```
qos cos default-cos
no qos cos
```
- **default-cos**—Specifies the default CoS value being assigned to the port. If the port is trusted and the packet is untagged then the default CoS value becomes the CoS value. (Range: 0 - 7)

**Default Configuration**
Port CoS is 0.

**Command Mode**
Interface Configuration (Ethernet, port-channel) command

**User Guidelines**
- You can use the default value to assign a CoS value to all untagged packets entering the port.

**Example**
The following example configures port g5 default CoS value to 3.

```
Console (config)# interface ethernet g5
Console (config-if) qos cos 3
```

**show qos map**
The show qos map User EXEC mode command displays all the QoS maps.

**Syntax**
```
show qos map [dscp-queue]
```
- dscp-queue—Displays the DSCP to queue map.

**Default Configuration**
This command has no default configuration.

**Command Mode**
User EXEC mode

**User Guidelines**
- There are no user guidelines for this command.
Example

The following example displays the DSCP port-queue map.

```
console# show qos map
Dscp-queue map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
---------------------------------------
 0 : 01 01 01 01 01 01 01 01 01 01
 1 : 01 01 01 01 01 01 02 02 02 02
 2 : 02 02 02 02 02 02 02 02 02 02
 3 : 02 02 03 03 03 03 03 03 03 03
 4 : 03 03 03 03 03 03 03 03 03 03
 5 : 04 04 04 04 04 04 04 04 04 04
 6 : 04 04 04 04
```

The following table describes the fields used above.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>Decimal Bit 1 of DSCP</td>
</tr>
<tr>
<td>D2</td>
<td>Decimal Bit 2 of DSCP</td>
</tr>
<tr>
<td>01 - 04</td>
<td>Queue numbers</td>
</tr>
</tbody>
</table>

\[(D1 \times 10) + D2 = \text{Value of DSCP}\]
Radius Commands

radius-server host

The `radius-server host` Global Configuration mode command specifies a RADIUS server host. To delete the specified RADIUS host, use the `no` form of this command.

Syntax

```
radius-server host {ip-address | hostname} [auth-port auth-port-number] [timeout timeout] [retransmit retransmit] [deadtime deadtime] [key] [source source] [priority priority] [usage type]

no radius-server host ip-address
```

- `ip-address`—IP address of the RADIUS server host.
- `hostname`—Hostname of the RADIUS server host. (Range: 1 - 158 characters)
- `auth-port-number`—Port number for authentication requests. The host is not used for authentication if set to 0. If unspecified, the port number defaults to 1812. (Range: 0 - 65535)
- `timeout`—Specifies the timeout value in seconds. If no timeout value is specified, the global value is used. (Range: 1 - 30)
- `retransmit`—Specifies the re-transmit value. If no re-transmit value is specified, the global value is used. (Range: 1 - 10)
- `deadtime`—Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests. (Range 0 - 2000)
- `key`—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. If no key value is specified, the global value is used. (Range: 1 - 128 characters)
- `source`—Specifies the source IP address to use for the communication. If no retransmit value is specified, the global value is used. 0.0.0.0 is interpreted as request to use the IP address of the outgoing IP interface.
- `priority`—Determines the order in which the servers are used, where 0 is the highest priority. (Range: 0 - 65535)
- `type`—Specifies the usage type of the server. Can be one of the following values: `login`, `802.1x` or `all`. If unspecified, defaults to `all`.

Default Configuration

By default, no RADIUS host is specified.
Command Mode
Global Configuration mode

User Guidelines
- To specify multiple hosts, multiple `radius-server host` commands can be used.
- If no host-specific timeout, retransmit, deadtime or key values are specified, the global values apply to each host.
- The address type of the source parameter must be the same as the ip-address parameter.

Example
The following example specifies a RADIUS server host with the following characteristics:
- Server host IP address—192.168.10.1
- Authentication port number—20
- Timeout period—20 seconds

```
Console (config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

`radius-server key`

The `radius-server key` Global Configuration mode command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. To reset to the default, use the `no` form of this command.

Syntax
```
radius-server key [key-string]
```
```
no radius-server key
```

- **key-string**—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. The key can be up to 128 characters long.

Default Configuration
The default is an empty string.

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.
Example
The following example sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon to "dell-server".

```
Console (config)# radius-server key dell-server
```

radius-server retransmit

The `radius-server retransmit` Global Configuration mode command specifies the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the `no` form of this command.

**Syntax**
```
radius-server retransmit retries
```
```
no radius-server retransmit
```
- `retries`—Specifies the retransmit value. (Range: 1 - 10)

**Default Configuration**
The default is 3 attempts.

**Command Mode**
Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example configures the number of times the software searches the list of RADIUS server hosts to 5 attempts.

```
Console (config)# radius-server retransmit 5
```

radius-server source-ip

The `radius-server source-ip` Global Configuration mode command specifies the source IP address used for communication with RADIUS servers. To return to the default, use the `no` form of this command.

**Syntax**
```
radius-server source-ip source
```
```
no radius-server-ip source
```
- `source`—Specifies the source IP address.
Default Configuration
The default IP address is the outgoing IP interface.

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example configures the source IP address used for communication with RADIUS servers to 10.1.1.1.

```console
Console (config)# radius-server source-ip 10.1.1.1
```

radius-server timeout
The `radius-server timeout` Global Configuration mode command sets the interval for which a device waits for a server host to reply. To restore the default, use the `no` form of this command.

Syntax
```
radius-server timeout timeout
no radius-server timeout
```
- `timeout`—Specifies the timeout value in seconds. (Range: 1 - 30)

Default Configuration
The default value is 3 seconds.

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example sets the interval for which a device waits for a server host to reply to 5 seconds.

```console
Console (config)# radius-server timeout 5
```
**radius-server deadtime**

The `radius-server deadtime` Global Configuration mode command improves RADIUS response times when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To reset the default value, use the `no` form of this command.

**Syntax**
- `radius-server deadtime deadtime`
- `no radius-server deadtime`

  - `deadtime`—Length of time in minutes, for which a RADIUS server is skipped over by transaction requests. (Range: 0 - 2000)

**Default Configuration**
The default dead time is 0 minutes.

**Command Mode**
Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example sets a dead time where a RADIUS server is skipped over by transaction requests for this period, to 10 minutes.

```
Console (config) # radius-server deadtime 10
```

**show radius-servers**
The `show radius-servers` User EXEC mode command displays the RADIUS server settings.

**Syntax**
- `show radius-servers`

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- There are no user guidelines for this command.
**Examples**

The following example displays the RADIUS server settings.

```plaintext
Console# show radius-servers

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>Time</th>
<th>Retransmit</th>
<th>Dead</th>
<th>Source</th>
<th>Priority</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Auth</td>
<td>Out</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.16.1.1</td>
<td>1645</td>
<td>Global</td>
<td>Global</td>
<td>Global</td>
<td>Global</td>
<td>1</td>
<td>All</td>
</tr>
<tr>
<td>172.16.1.2</td>
<td>1645</td>
<td>11</td>
<td>8</td>
<td>Global</td>
<td>Global</td>
<td>2</td>
<td>All</td>
</tr>
</tbody>
</table>

Global values
--------------
Timeout: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```
RMON Commands

show rmon statistics

The show rmon statistics User EXEC mode command displays RMON Ethernet Statistics.

Syntax

show rmon statistics {ethernet interface number | port-channel port-channel-number}

- interface—Valid Ethernet port.
- port-channel-number—Valid port-channel trunk index.

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
- The following RMON Groups are supported - Ethernet Statistics (Group 1), History (Group 2), Alarms (Group 3) and Events (Group 4).

Example

The following example displays RMON Ethernet Statistics for port g1.

```console
Console# show rmon statistics ethernet g1
Port g1
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```
The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped</td>
<td>The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The total number of good packets received and directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast</td>
<td>The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>CRC Align Errors</td>
<td>The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Undersize Pkts</td>
<td>The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Oversize Pkts</td>
<td>The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>64 Octets</td>
<td>The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>65 to 127 Octets</td>
<td>The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>128 to 255 Octets</td>
<td>The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
rmon collection history

The `rmon collection history` Interface Configuration mode command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the `no` form of this command.

**Syntax**

```
 rmon collection history index [owner ownername] [buckets bucket-number] [interval seconds]

 no rmon collection history index
```

- `index`—The requested statistics index group. (Range: 1 - 65535)
- `owner ownername`—Records the RMON statistics group owner name. If unspecified, the name is an empty string.
- `buckets bucket-number`—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1 - 65535)
- `interval seconds`—The number of seconds in each polling cycle. If unspecified, defaults to 1800. (Range: 1 - 3600)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- This command cannot be executed on multiple ports using the `interface range ethernet` command.

<table>
<thead>
<tr>
<th>Octet Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 to 511 Octets</td>
<td>The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>512 to 1023 Octets</td>
<td>The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>1024 to 1518 Octets</td>
<td>The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
Example
The following example enables a Remote Monitoring (RMON) MIB history statistics group on port g8 with the index number "1" and a polling interval period of 2400 seconds.

```
Console (config)# interface ethernet g8
Console (config-if)# rmon collection history 1 interval 2400
```

**show rmon collection history**
The `show rmon collection history` User EXEC mode command displays the requested history group configuration.

**Syntax**

```
show rmon collection history [ethernet interface | port-channel port-channel-number]
```
- `interface`—Valid Ethernet port.
- `port-channel-number`—Valid port-channel trunk index.

**Default Configuration**
This command has no default configuration.

**Command Mode**
User EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example displays all RMON group statistics.

```
Console# show rmon collection history

+-----+----------+---------+----------+---------+--------+
<p>|Index| Interface| Interval| Requested| Granted |</p>
<table>
<thead>
<tr>
<th>-----</th>
<th>----------</th>
<th>---------</th>
<th>----------</th>
<th>---------</th>
<th>--------</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1000</td>
<td>50</td>
<td>50</td>
<td>CLI</td>
</tr>
</tbody>
</table>
```


The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The sampled Ethernet interface</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds between samples.</td>
</tr>
<tr>
<td>Requested Samples</td>
<td>The requested number of samples to be saved.</td>
</tr>
<tr>
<td>Granted Samples</td>
<td>The granted number of samples to be saved.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>

**show rmon history**

The `show rmon history` User EXEC mode command displays RMON Ethernet Statistics history.

**Syntax**

```
show rmon history index {throughput | errors | other} [period seconds]
```

- `index`—The requested set of samples. (Range: 1 - 65535)
- `throughput`—Displays throughput counters.
- `errors`—Displays error counters.
- `other`—Displays drop and collision counters.
- `period seconds`—Specifies the requested period time to display. (Range: 1 - 4294967295)

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode

**User Guidelines**

- There are no user guidelines for this command.
Examples

The following example displays RMON Ethernet Statistics history for "throughput" on index number 5.

```
Console# show rmon history 5 throughput
Sample Set: 1               Owner: CLI
Interface: g1               Interval: 1800
Requested samples: 50       Granted samples: 50

Maximum table size: 500

<table>
<thead>
<tr>
<th>Time</th>
<th>Octets</th>
<th>Packets</th>
<th>Broadcast</th>
<th>Multicast</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18 2002 21:57:00</td>
<td>303595962</td>
<td>357568</td>
<td>3289</td>
<td>7287</td>
<td>19.98%</td>
</tr>
<tr>
<td>Jan 18 2002 21:57:30</td>
<td>287696304</td>
<td>275686</td>
<td>2789</td>
<td>2789</td>
<td>20.17%</td>
</tr>
</tbody>
</table>
```

The following example displays RMON Ethernet Statistics history for "errors" on index number 5.

```
Console# show rmon history 5 errors
Sample Set: 1               Owner: CLI
Interface: g1               Interval: 1800
Requested samples: 50       Granted samples: 50

Maximum table size: 500

<table>
<thead>
<tr>
<th>Time</th>
<th>CRC Align</th>
<th>Undersize</th>
<th>Oversize</th>
<th>Fragments</th>
<th>Jabbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18 2002 21:57:00</td>
<td>1</td>
<td>1</td>
<td>49</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 18 2002 21:57:30</td>
<td>1</td>
<td>1</td>
<td>27</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following example displays RMON Ethernet Statistics history for "other" on index number 5.

```
```
The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and Time the entry is recorded.</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>The number of packets (including bad packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The number of good packets received during this sampling interval that were directed to the broadcast address.</td>
</tr>
<tr>
<td>Multicast</td>
<td>The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.</td>
</tr>
<tr>
<td>Utilization%</td>
<td>The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
<tr>
<td>CRC Align</td>
<td>The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Undersize</td>
<td>The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
</tbody>
</table>
The `rmon alarm` Global Configuration mode command configures alarm conditions. To remove an alarm, use the `no` form of this command.

**Syntax**

```
rmon alarm index variable interval rthreshold fthreshold revent fevent [type type] [startup direction] [owner name]
```

```
no rmon alarm index
```

- `index`—The alarm index. (Range: 1 - 65535)
- `variable`—The object identifier of the particular variable to be sampled.
- `interval`—The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1 - 2147483648)
- `rthreshold`—Rising Threshold. (Range: 1 - 4294967295)
- `fthreshold`—Falling Threshold. (Range: 1 - 4294967295)
- `revent`—The Event index used when a rising threshold is crossed. (Range: 1 - 65535)
- `fevent`—The Event index used when a falling threshold is crossed. (Range: 1 - 65535)

### Table: Alarm Conditions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversize</td>
<td>The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Dropped</td>
<td>The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.</td>
</tr>
</tbody>
</table>
• **type** *type*—The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.

• **startup direction**—The alarm that may be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the **r**threshold, and *direction* is equal to **rising** or **rising-falling**, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the **f**threshold, and *direction* is equal to **falling** or **rising-falling**, then a single falling alarm is generated.

• **owner name**—Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

**Default Configuration**

The following parameters have the following default values:

• **type** *type*—If unspecified, the type is **absolute**.

• **startup direction**—If unspecified, the startup direction is **rising-falling**.

**Command Mode**

Global Configuration mode

**User Guidelines**

• There are no user guidelines for this command.

**Example**

The following example configures the following alarm conditions:

• Alarm index—1000
• Variable identifier—dell
• Sample interval—360000 seconds
• Rising threshold—1000000
• Falling threshold—1000000
• Rising threshold event index—10
• Falling threshold event index—20

```
Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20
```

**show rmon alarm-table**

The show **rmon alarm-table** User EXEC mode command displays the alarms summary table.
Syntax

show rmon alarm-table

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

• There are no user guidelines for this command.

Example

The following example displays the alarms summary table.

```
Console# show rmon alarm-table

<table>
<thead>
<tr>
<th>Index</th>
<th>OID</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.3.6.1.2.1.2.2.1.10.1</td>
<td>CLI</td>
</tr>
<tr>
<td>2</td>
<td>1.3.6.1.2.1.2.1.10.1</td>
<td>Manager</td>
</tr>
<tr>
<td>3</td>
<td>1.3.6.1.2.1.2.1.10.9</td>
<td>CLI</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>

**show rmon alarm**

The `show rmon alarm` User EXEC mode command displays alarm configuration.

Syntax

```
show rmon alarm number
```

• `number`—Alarm index. (Range: 1 - 65535)
Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example displays RMON 1 alarms.

```
Console# show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Last Sample Value</td>
<td>The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Alarm index.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>
The `rmon event` Global Configuration mode command configures an event. To remove an event, use the `no` form of this command.

**Syntax**

```
rmon event index type [community text] [description text] [owner name]
```

- **index**—The event index. (Range: 1 - 65535)
- **type**—The type of notification that the device generates about this event. Can have the following values: `none`, `log`, `trap`, `log-trap`. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
- **community text**—If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- **description text**—A comment describing this event. (Range: 0-127 characters)
- **owner name**—Enter a name that specifies who configured this event. If unspecified, the name is an empty string. (Range: 0-127 characters)

<table>
<thead>
<tr>
<th>Interval</th>
<th>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Type</td>
<td>The method of sampling the variable and calculating the value compared against the thresholds. If the value is <code>absolute</code>, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is <code>delta</code>, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</td>
</tr>
<tr>
<td>Startup Alarm</td>
<td>The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.</td>
</tr>
<tr>
<td>Rising Threshold</td>
<td>A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.</td>
</tr>
<tr>
<td>Falling Threshold</td>
<td>A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.</td>
</tr>
<tr>
<td>Rising Event</td>
<td>The event index used when a rising threshold is crossed.</td>
</tr>
<tr>
<td>Falling Event</td>
<td>The event index used when a falling threshold is crossed.</td>
</tr>
</tbody>
</table>
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example configures an event with the trap index of 10.

```
Console (config)# rmon event 10 log
```

show rmon events
The show rmon events User EXEC mode command displays the RMON event table.

Syntax
```
show rmon events
```

Default Configuration
This command has no default configuration.

Command Mode
User EXEC mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example displays the RMON event table.
The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing this event.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of notification that the device generates about this event. Can have the following values: none, log, trap, log-trap. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.</td>
</tr>
<tr>
<td>Community</td>
<td>If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this event.</td>
</tr>
<tr>
<td>Last time sent</td>
<td>The time this entry last generated an event. If this entry has not generated any events, this value is zero.</td>
</tr>
</tbody>
</table>

**show rmon log**

The `show rmon log` User EXEC mode command displays the RMON logging table.

**Syntax**

```
show rmon log [event]
```

- `event`—Event index. (Range: 0 - 65535)

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode
User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the RMON logging table.

```
Console# show rmon log

Maximum table size: 500

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Errors</td>
<td>Jan 18 2002 23:48:19</td>
</tr>
<tr>
<td>1</td>
<td>Errors</td>
<td>Jan 18 2002 23:58:17</td>
</tr>
<tr>
<td>2</td>
<td>High Broadcast</td>
<td>Jan 18 2002 23:59:48</td>
</tr>
</tbody>
</table>

Console# show rmon log

Maximum table size: 500 (800 after reset)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Errors</td>
<td>Jan 18 2002 23:48:19</td>
</tr>
<tr>
<td>1</td>
<td>Errors</td>
<td>Jan 18 2002 23:58:17</td>
</tr>
<tr>
<td>2</td>
<td>High Broadcast</td>
<td>Jan 18 2002 23:59:48</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>An index that uniquely identifies the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing this event.</td>
</tr>
<tr>
<td>Time</td>
<td>The time this entry created.</td>
</tr>
</tbody>
</table>
rmon table-size

The rmon table-size Global Configuration mode command configures the maximum RMON tables sizes. To return to the default configuration, use the no form of this command.

Syntax

```
rmon table-size {history entries | log entries}
no rmon table-size {history | log}
```

- **history entries**—Maximum number of history table entries. (Range: 20 - 32767)
- **log entries**—Maximum number of log table entries. (Range: 20 - 32767)

Default Configuration

History table size is 270.
Log table size is 200.

Command Mode

Global Configuration mode

User Guidelines

- The configured table size is effective after the device is rebooted.

Example

The following example configures the maximum RMON history table sizes to 1000 entries.

```
Console (config)# rmon table-size history 1000
```
SNMP Commands

**snmp-server community**

Use the `snmp-server community` command to set up the community access string to permit access to the Simple Network Management Protocol command. Use the `no` form of this command removes the specified community string.

**Syntax**

```
snmp-server community community [ro | rw | su] [ip-address] [view view-name]
```

```
snmp-server community-group community-group-name [ip-address]
```

```
o snmp-server community community [ip-address]
```

- `community` — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 chars)
- `ro` — Specifies read-only access (Default)
- `rw` — Specifies read-write access
- `su` — Specifies SNMP administrator access
- `view view-name` — Name of a previously defined view. The view defines the objects available to the community. It’s not relevant for `su`, which has access to the whole MIB. If unspecified, all the objects except of the community-table and SNMPv3 user and access tables are available. (Range: 1-30 chars)
- `ip-address` — Management station IP address. Default is all IP addresses. An out-of-band IP address can be specified as described in the usage guidelines. (Range: Valid IP address)
- `group-name` — Name of a previously defined group. The group defines the objects available to the community. (Range: 1-30 chars)

**Default Configuration**

There are no default communities defined.

**Command Mode**

Global Configuration mode

**User Guidelines**

- You can’t specify view-name for `su`, which has an access to the whole MIB.
- You can use the `view-name` to restrict the access rights of a community string.
  
  By specifying the `view-name` parameter the software:
  
  1. Generates an internal security-name.
2 Map the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.

3 Map the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also)

- You can use the group-name to restrict the access rights of a community string. By specifying the group-name parameter the software:
  1 Generates an internal security-name.
  2 Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Examples
The following example sets up the community access string "public" to permit administrative access to SNMP protocol, at an administrative station with the IP address 192.168.1.20.

```
Console (config)# snmp-server community public su 192.168.1.20
```

**snmp-server view**

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no** form of this command.

**Syntax**

```
snmp-server view view-name oid-tree {included | excluded}

no snmp-server view view-name [oid-tree]
```

- **view-name** — Label for the view record that you are updating or creating. The name is used to reference the record. (Range: 1 - 30 chars)
- **oid-tree** — Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as `system`. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included** — The view type is included.
- **excluded** — The view type is excluded.

**Default Setting**

"Default" and "DefaultSuper" views exists.

**Command Mode**

Global configuration
User Guidelines

- You can enter this command multiple times for the same view record.
- The number of views is limited to 64.
- "Default" and "DefaultSuper" views exist. Those views are used by the software internally and can't be deleted or modified.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
Console (config)# snmp-server view user-view system included
Console (config)# snmp-server view user-view system.7 excluded
Console (config)# snmp-server view user-view ifEntry.*.1 include
```

snmp-server filter

To create or update a filter entry, use the `snmp-server filter` global configuration command. To remove the specified Simple Network Management Protocol (SNMP) server filter entry, use the `no` form of this command.

**Syntax**

```
snmp-server filter filter-name oid-tree {included | excluded}
no snmp-server filter filter-name [oid-tree]
```

- `filter-name` — Label for the filter record that you are updating or creating. The name is used to reference the record. (Range: Up to 30 characters).
- `oid-tree` — Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as `system`. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- `included` — The filter type is included.
- `excluded` — The filter type is excluded.

**Default Configuration**

Product specific.

**Command Modes**

Global Configuration
You can enter this command multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
Console (config)# snmp-server view user-view system included
Console (config)# snmp-server view user-view system.7 excluded
Console (config)# snmp-server view user-view ifEntry.*.1 included
```

**snmp-server contact**

The `snmp-server contact` Global Configuration mode command sets up a system contact. To remove the system contact information, use the `no` form of the command.

**Syntax**

```
   snmp-server contact text
   no snmp-server contact
```

- `text`—Character string, up to 160 characters, describing the system contact information.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

- Do not include spaces in the text string.

**Example**

The following example displays setting up the system contact point as "Dell_Technical_Support".

```
Console (config)# snmp-server contact Dell_Technical_Support
```

**snmp-server location**

The `snmp-server location` Global Configuration mode command sets up information on where the device is located. To remove the location string use, the `no` form of this command.
Syntax

  snmp-server location text
  no snmp-server location
  •  text—Character string, up to 160 characters, describing the system location.

Default Configuration

  This command has no default configuration.

Command Mode

  Global Configuration mode

User Guidelines

  •  Do not include spaces in the text string.

Example

  The following example sets the device location as "New_York".

  Console (config)# snmp-server location New_York

snmp-server enable traps

  The snmp-server enable traps Global Configuration mode command enables the switch to send SNMP traps. To disable SNMP traps use the no form of the command.

Syntax

  snmp-server enable traps
  no snmp-server enable traps

Default Configuration

  Enabled

Command Mode

  Global Configuration mode

User Guidelines

  •  There are no user guidelines for this command.

Examples

  The following example displays the command to enable SNMP traps.

  Console (config)# snmp-server enable traps
**snmp-server trap authentication**

The **snmp-server trap authentication** Global Configuration mode command enables the switch to send Simple Network Management Protocol traps when authentication fails. To disable SNMP authentication failed traps, use the **no** form of this command.

**Syntax**

```
snmp-server trap authentication
no snmp-server trap authentication
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example displays the command to enable authentication failed SNMP traps.

```
Console (config)# snmp-server trap authentication
```

---

**snmp-server host**

To specify the recipient of Simple Network Management Protocol notification operation, use the **snmp-server host** global configuration command. Use the **no** form of this command to remove the specified host.

**Syntax**

```
snmp-server host {ip-address | hostname} community-string [traps | informs] [1 | 2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]
no snmp-server host {ip-address | hostname} [traps | informs]
```

- **ip-address** — Internet address of the host (the targeted recipient). An out-of-band IP address can be specified as described in the usage guidelines.
- **hostname** — Hostname of the host. (Range: 1 - 158 characters).
- **community-string** — Password-like community string sent with the notification operation. (Range: 1 - 20 chars)
- **traps** — Sends SNMP traps to this host (Default).
- **informs** — Sends SNMP informs to this host. Not applicable to SNMPv1.
• 1 — SNMPv1 traps will be used.
• 2 — SNMPv2 traps will be used (Default).
• udp-port port — UDP port of the host to use. The default is 162. (Range: 1 - 65535)
• filter filtername — A string that is the name of the filter that define the filter for this host. If unspecified, does not filter anything. (Range : Up to 30 characters).
• timeout seconds — Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range :1 - 300)
• retries retries — Maximum number of times to resend an inform request, when response is not received for generated message. The default is 3. (Range: 0 - 255)

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
• When configuring snmp v1 or v2 notification recipients, the software should automatically generate notification views for those recipients, for all MIBs.

Example
The following example specifies the recipient of Simple Network Management Protocol notification operation.

```
Console (config)# snmp-server host 10.1.1.1 management 2
```

`snmp-server set`
The `snmp-server set` Global Configuration mode command sets SNMP MIB value by the CLI.

Syntax
```
snmp-server set variable-name name1 value1 [name2 value2 ...]
```
• `variable-name` — MIB variable name.
• `name value`.— List of name and value pairs. In case of scalar MIBs there is only a single pair of name values. In case of entry in a table the first pairs are the indexes, followed by one or more fields.

Default Configuration
This command has no default configuration.
Command Mode

Global Configuration mode

User Guidelines

- Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the `snmp-server set` command is used.
- This command is context sensitive.

Examples

The following example sets the scalar MIB "sysName" to have the value "dell".

```
Console (config)# snmp-server set sysName sysname dell
```

The following example sets the entry MIB "rndCommunityTable" with keys 0.0.0.0 and "public". The field `rndCommunityAccess` gets the value "super" and the rest of the fields get their default values.

```
Console (config)# snmp-server set rndCommunityTable
rndCommunityMngStationAddr 0.0.0.0 rndCommunityString public
rndCommunityAccess super
```

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the `snmp-server group` global configuration command. To remove a specified SNMP group, use the no form of this command.

Syntax

```
no snmp-server group groupname [v1 | v2 | v3 [noauth | auth | priv] [notify notifyview | ] [context name] [read readview] [write writeview]
```

- `groupname` — The name of the group. (Range: Up to 30 characters)
- `v1` — SNMP Version 1 security model.
- `v2` — SNMP Version 2 security model.
- `v3` — SNMP Version 3 security model.
- `noauth` — Specifies no authentication of a packet. Applicable only to SNMP Version 3 security model.
- `auth` — Specifies authentication of a packet without encrypting it. Applicable only to SNMP Version 3 security model.
• **priv** — Specifies authentication of a packet with encryption. Applicable only to SNMP Version 3 security model.

• **context name** — Specifies context of packet.

• **read readview** — A string that is the name of the view that enables you only to view the contents of the agent. If unspecified, all the objects except of the community-table and SNMPv3 user and access tables are available. (Range: Up to 30 characters)

• **write writeview** — A string that is the name of the view that enables you to enter data and configure the contents of the agent. If unspecified, nothing is defined for the write view. (Range: Up to 30 characters)

• **notify notifyview** — A string that is the name of the view that enables you to specify an inform or a trap. If unspecified, nothing is defined for the notify view. (Range: Up to 30 characters)

**Default configuration**

No group entry exists.

**Command Mode**

Global configuration

**User Guidelines**

• The Router context is translated to "**" context in the MIB.

**Example**

The following example configures a new Simple Network Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views

```
Console (config)# snmp-server group user-group v3 priv read
user-view
```

**snmp-server user**

To configure a new SNMP Version 3 user, use the `snmp-server user` global configuration command. To remove a user, use the `no` form of the command.

**Syntax**

```
snmp-server user username groupname [remote engineid-string] [ auth-md5 password | auth-sha password | auth-md5-key md5-des-keys | auth-sha-key sha-des-keys ]

no snmp-server user username [remote engineid-string ]
```

• **username** — The name of the user on the host that connects to the agent. (Range: Up to 30 characters)
- **groupname** — The name of the group to which the user belongs. (Range: Up to 30 characters)

- **remote engineid-string** — Specifies the engine ID of remote SNMP entity to which the user belongs. The engine ID is concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 5 - 32 characters)

- **auth-md5** — The HMAC-MD5-96 authentication level. The user should enter password.

- **auth-sha** — The HMAC-SHA-96 authentication level. The user should enter password.

- **password** — A password (not to exceed 32 characters) for authentication and generation of DES key for privacy. (Range: Up to 30 characters)

- **auth-md5-key** — The HMAC-MD5-96 authentication level. The user should enter authentication and privacy keys.

- **md5-des-keys** — Concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is only required you should enter 16 bytes, if authentication and privacy are required you should enter 32 bytes. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 16 - 32 characters)

- **auth-sha-key** — The HMAC-SHA-96 authentication level. The user should enter authentication and privacy keys.

- **sha-des-keys** — Concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required you should enter 20 bytes, if authentication and privacy are required you should enter 36 bytes. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 20 - 36 characters)

**Default configuration**

No group entry exists.

**Command Mode**

Global configuration

**User Guidelines**

- If **auth-md5** or **auth-sha** is specified, both authentication and privacy are enabled for the user.

  When you enter a `show running-config` command, you will not see a line for this user. To see if this user has been added to the configuration, type the `show snmp user` command.

  An SNMP EngineID should be defined in order to add users to the device.

  Changing or removing the value of snmpEngineID deletes the SNMPv3 users database.
Example
The following example configures a new SNMP Version 3 user.

```
Console (config)# snmp-server user
```

**snmp-server v3-host**
The `snmp-server v3-host` Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the `no` form of this command.

**Syntax**
```
snmp-server v3-host {ip-address | hostname} username [traps | informs] {noauth | auth | priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

```
no snmp-server host {ip-address | hostname} username [traps | informs]
```

- `ip-address`—Specifies the IP address of the host (targeted recipient).
- `hostname`—Specifies the name of the host. (Range: 1-158 characters).
- `username`—Specifies the name of the user to use to generate the notification. (Range: 1-24)
- `traps`—Indicates that SNMP traps are sent to this host.
- `informs`—Indicates that SNMP informs are sent to this host.
- `noauth`—Indicates no authentication of a packet.
- `auth`—Indicates authentication of a packet without encrypting it.
- `priv`—Indicates authentication of a packet with encryption.
- `port`—Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
- `filtername`—Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- `seconds`—Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
- `retries`—Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 1-255)

**Default Setting**
This command has no default configuration.
**Command Mode**
Global Configuration mode

**User Guidelines**
- A user and notification view are not automatically created. Use the `snmp-server user`, `snmp-server group` and `snmp-server view` Global Configuration mode commands to generate a user, group and notify group, respectively.

**Example**
The following example configures an SNMPv3 host.

```
Console(config)# snmp-server v3-host 192.168.0.20 john noauth
```

**snmp-server engineID local**
The `snmp-server engineID local` Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. To remove the configured engine ID, use the `no` form of this command.

**Syntax**
```
snmp-server engineID local {engineid-string | default}
```
```
no snmp-server engineID local
```
- `engineid-string` — Specifies a character string that identifies the engine ID. (Range: 5-32 characters)
- `default` — The engine ID is created automatically based on the device MAC address.

**Default Setting**
The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:
- First 4 octets — first bit = 1, the rest is IANA Enterprise number.
- Fifth octet — set to 3 to indicate the MAC address that follows.
- Last 6 octets — MAC address of the device.

**Command Mode**
Global Configuration mode

**User Guidelines**
- To use SNMPv3, you have to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device.
If the SNMPv3 engine ID is deleted or the configuration file is erased, SNMPv3 cannot be used. By default, SNMPv1/v2 are enabled on the device. SNMPv3 is enabled only by defining the Local Engine ID.

If you want to specify your own ID, you do not have to specify the entire 32-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up to the point where just zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify snmp-server engineID local 1234.

Since the engine ID should be unique within an administrative domain, the following is recommended:

- For a standalone device, use the default keyword to configure the engine ID.
- For a stackable system, configure the engine ID and verify its uniqueness.

Changing the value of the engine ID has the following important side-effect. A user’s password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The user’s command line password is then destroyed, as required by RFC 2274. As a result, the security digests of SNMPv3 users become invalid if the local value of the engine ID change, and the users will have to be reconfigured.

You cannot specify an engine ID that consists of all 0x0, all 0xF or 0x000000001.

The show running-config Privileged EXEC mode command does not display the SNMP engine ID configuration. To see the SNMP engine ID configuration, enter the snmp-server engine ID local GlobalConfiguration mode command.

**Example**

The following example specifies the Simple Network Management Protocol (SNMP) engineID on the local device.

```
Console(config) # snmp-server engineID local default
```

**show snmp engineid**

The show snmp engineID Privileged EXEC mode command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

**Syntax**

```
show snmp engineID
```

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode
User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the SNMP engine ID.

```
Console# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
```

**show snmp**

The `show snmp` Privileged EXEC mode command displays the SNMP status.

Syntax

```
show snmp
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the SNMP communications status.

```
console# sh snmp
```
Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Community</th>
<th>Version</th>
<th>UDP Port</th>
<th>Filter</th>
<th>TO Security</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version 3 notifications

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Username</th>
<th>Security</th>
<th>UDP Port</th>
<th>Filter</th>
<th>TO Security</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

System Contact:

System Location:

```
console#
```

**show snmp views**

To display the configuration of views use the **show snmp views** Privileged EXEC command

**Syntax**

```
show snmp views [viewname]
```

- **viewname**— The name of the view. Range: Up to 30 characters

Default Configuration

There is no default configuration for this command.

**Command Modes**

Privileged EXEC

**User Guidelines**

- There are no user guidelines for this command

**Example**

The following example displays the configuration of views use the show snmp views Privileged EXEC command.
To display the configuration of groups use the `show snmp groups` Privileged EXEC command.

**Syntax**

```
show snmp groups [groupname]
```

- `groupname` — The name of the group.

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

- Privileged EXEC

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the configuration of views use the `show snmp views` Privileged EXEC command.
show snmp groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Security Model</th>
<th>Security Level</th>
<th>Security Context</th>
<th>Read View</th>
<th>Write View</th>
<th>Notify View</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-group</td>
<td>V3</td>
<td>priv</td>
<td>-</td>
<td>Default</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>managers-group</td>
<td>V3</td>
<td>priv</td>
<td>-</td>
<td>Default</td>
<td>Default</td>
<td>-</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3</td>
<td>priv</td>
<td>-</td>
<td>Default</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Console # show snmp groups user-group

Name: user-group
Security Model: V3
Security Level: priv
Security Context: -
Read View: Default
Write View: ""
Notify View: ""

**show snmp filters**

To display the configuration of filters use the **show snmp filters** Privileged EXEC command.

**Syntax**

```
show snmp filters [filtername]
```

- `filtername` — The name of the view. Range: Up to 30 character

**Default Configuration**

There is no default configuration for this command.
**Command Modes**

Privileged EXEC

**User Guidelines**

- There are no user guidelines for this command

**Example**

The following example displays the configuration of filters use the show snmp filters Privileged EXEC command.

```
Console # show snmp filters

<table>
<thead>
<tr>
<th>Name</th>
<th>OID Tree</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.1</td>
<td>Included</td>
</tr>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.1.7</td>
<td>Excluded</td>
</tr>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.2.1.* .1</td>
<td>Included</td>
</tr>
</tbody>
</table>
```

**show snmp users**

To display the configuration of groups use the show snmp users Privileged EXEC command.

**Syntax**

```
show snmp users [username]
```

- **username** — The name of the user. Range: Up to 30 character

**Default Configuration**

There is no default configuration for this command.

**Command Modes**

Privileged EXEC

**User Guidelines**

- There are no user guidelines for this command

**Example**

The following example displays the configuration of groups use the show snmp users Privileged EXEC command.
Console # show snmp users

<table>
<thead>
<tr>
<th>Name</th>
<th>group name</th>
<th>Auto Method</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>1.3.6.1.2.1.1</td>
<td>md5</td>
<td></td>
</tr>
<tr>
<td>John</td>
<td>1.3.6.1.2.1.1.7</td>
<td>md5</td>
<td>08009009020C0B099C075879</td>
</tr>
</tbody>
</table>

Console # show snmp users John

Name: John
Group name: user-group
Auth Method: md5
Remote:

Name: John
Group name: user-group
Auth Method: md5
Remote: 08009009020C0B099C075879
Spanning-Tree Commands

**spanning-tree**
The `spanning-tree` Global Configuration mode command enables spanning-tree functionality. To disable spanning-tree functionality, use the `no` form of this command.

**Syntax**
```
spanning-tree

no spanning-tree
```

**Default Configuration**
Spanning-tree is enabled.

**Command Modes**
- Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

**spanning-tree mode**
The `spanning-tree mode` Global Configuration mode command configures the spanning-tree protocol. To return to the default configuration, use the `no` form of this command.

**Syntax**
```
spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode
```

- `stp`—STP is the Spanning Tree operative mode.
- `rstp`—RSTP is the Spanning Tree operative mode.
- `mstp`—MSTP is enabled

**Default Configuration**
STP
Command Modes

Global Configuration mode

User Guidelines

- In RSTP mode, the switch would use STP when the neighbor switch is using STP.
- In MSTP mode the switch would use RSTP when the neighbor switch is using RSTP, and would use STP when the neighbor switch is using STP.

Example

The following example configures the spanning-tree protocol to RSTP.

```console
Console(config)# spanning-tree mode rstp
```

spanning-tree forward-time

The `spanning-tree forward-time` Global Configuration mode command configures the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.

To reset the default forward time, use the `no` form of this command.

Syntax

```
spanning-tree forward-time seconds
no spanning-tree forward-time
```

- **seconds**—Time in seconds. (Range: 4 - 30)

Default Configuration

The default forwarding-time for IEEE Spanning-tree Protocol (STP) is 15 seconds.

Command Modes

Global Configuration mode

User Guidelines

- When configuring the Forward-Time the following relationship should be kept:
  - \(2^*(\text{Forward-Time} - 1) \geq \text{Max-Age}\)

Example

The following example configures spanning-tree bridge forward time to 25 seconds.

```console
Console(config)# spanning-tree forward-time 25
```
spanning-tree hello-time

The `spanning-tree hello-time` Global Configuration mode command configures the spanning-tree bridge hello time, which is how often the switch broadcasts hello messages to other switches. To reset the default hello time, use the `no` form of this command.
Syntax

spanning-tree hello-time seconds
no spanning-tree hello-time

- seconds—Time in seconds. (Range: 1 - 10)

Default Configuration

The default hello time for IEEE Spanning-Tree Protocol (STP) is 2 seconds.

Command Modes

Global Configuration mode

User Guidelines

- When configuring the Hello-Time the following relationship should be kept:
  - Max-Age $\geq 2^*$(Hello-Time + 1)

Example

The following example configures spanning-tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

spanning-tree max-age

The spanning-tree max-age Global Configuration mode command configures the spanning-tree bridge maximum age. To reset the default maximum age, use the no form of this command.

Syntax

spanning-tree max-age seconds
no spanning-tree max-age

- seconds—Time in seconds. (Range: 6 - 40)

Default Configuration

The default max-age for IEEE STP is 20 seconds.

Command Modes

Global Configuration mode

User Guidelines

- When configuring the Max-Age the following relationships should be kept:
  - $2^*$(Forward-Time - 1) $\geq$ Max-Age
  - Max-Age $\geq 2^*$(Hello-Time + 1)
Example
The following example configures the spanning-tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

**spanning-tree priority**

The `spanning-tree priority` Global Configuration mode command configures the spanning-tree priority. The priority value is used to determine which bridge is elected as the root bridge. To reset the default spanning-tree priority use the `no` form of this command.

**Syntax**
```
spanning-tree priority priority
no spanning-tree priority
```

- `priority`—Priority of the bridge. (Range: 0 - 65535 in steps of 4096)

**Default Configuration**
The default bridge priority for IEEE STP is 32768.

**Command Modes**
Global Configuration mode

**User Guidelines**
- The priority value must be a multiple of 4096.
- The bridge with the lowest priority is elected to be the Root Bridge.

**Example**
The following example configures spanning-tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

**spanning-tree disable**

The `spanning-tree disable` Interface Configuration mode command disables spanning-tree on a specific port. To enable spanning-tree on a port use, the `no` form of this command.

**Syntax**
```
spanning-tree disable
no spanning-tree disable
```

**Default Configuration**
By default, all ports are enabled for spanning-tree.
Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- When STP is disabled, the device will not forward STP BPDU’s based on the Forward BPDU’s setting.

Example

The following example disables spanning-tree on g5.

```
Console (config)# interface ethernet g5
Console (config-if)# spanning-tree disable
```

spanning-tree cost

The `spanning-tree cost` Interface Configuration mode command configures the spanning-tree path cost for a port. To reset the default port path cost, use the `no` form of this command.

Syntax

```
spanning-tree cost cost
no spanning-tree cost
```

- `cost`—The port path cost (Range: 1 - 200,000,000)

Default Configuration

For the default short pathcost method, the cost values are: port channel - 4; 1000 mbps - 4; 100 mbps - 19; 10 mbps - 100.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- The method used (long or short) is set by using the `spanning-tree pathcost method` command.

Example

The following example configures the spanning-tree cost on g5 to 35000.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree cost 35000
```
spanning-tree port-priority

The `spanning-tree port-priority` Interface Configuration mode command configures port priority. To reset the default port priority, use the `no` form of this command.

**Syntax**

```
spanning-tree port-priority priority
no spanning-tree port-priority
```

- `priority`—The port priority. (Range: 0 - 240 in multiples of 16)

**Default Configuration**

The default port-priority for IEEE STP is 128.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example configures the spanning priority on g5 to 96.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree port-priority 96
```

spanning-tree portfast

The `spanning-tree portfast` Interface Configuration mode command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. To disable PortFast mode, use the `no` form of this command.

**Syntax**

```
spanning-tree portfast
no spanning-tree portfast
```

**Default Configuration**

PortFast mode is disabled.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode
User Guidelines

- This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

Example

The following example enables PortFast on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree portfast
```

spanning-tree link-type

The `spanning-tree link-type` Interface Configuration mode command overrides the default link-type setting. To reset the default, use the `no` form of this command.

Syntax

```
spanning-tree link-type {point-to-point | shared}
```

```
no spanning-tree spanning-tree link-type
```

- `point-to-point`—Specifies the port link type as point-to-point.
- `shared`—Specifies that the port link type is shared.

Default Configuration

There is no default configuration for this command.

Command Modes

- Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

Example

The following example enables shared spanning-tree on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree link-type shared
```
**spanning-tree mst priority**

The **spanning-tree mst priority** Global Configuration mode command configures the device priority for the specified spanning-tree instance. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
spanning-tree mst instance-id priority priority
no spanning-tree mst instance-id priority
```

- **instance-id** — Displays the ID of the spanning-tree instance (Range: 1-15).
- **priority** — Displays the device priority for the specified spanning-tree instance (Range: 0-61440 in multiples of 4096).

**Default Setting**

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

**Command Mode**

Global Configuration mode

**User Guidelines**

- The device with the lowest priority is selected as the root of the spanning tree.

**Example**

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console (config) # spanning-tree mst 1 priority 4096
```

**spanning-tree mst max-hops**

The **spanning-tree mst priority** Global Configuration mode command configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
spanning-tree mst max-hops hop-count
no spanning-tree mst max-hops
```

- **hop-count** — Number of hops in an MST region before the BDPU is discarded. (Range: 1-40)

**Default Setting**

The default number of hops is 20.
Command Mode

Global Configuration mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console (config) # spanning-tree mst max-hops 10
```

spanning-tree mst port-priority

The `spanning-tree mst port-priority` Interface Configuration mode command configures port priority for the specified MST instance. To return to the default configuration, use the `no` form of this command.

Syntax

```
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

- `instance-ID` — ID of the spanning tree instance. (Range: 1-15)
- `priority` — The port priority. (Range: 0 - 240 in multiples of 16)

Default Setting

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example configures the port priority of port g1 to 142.

```
Console(config)# interface ethernet g1
Console(config-if)# spanning-tree mst 1 port-priority 142
```
spanning-tree mst cost

The `spanning-tree mst cost` Interface Configuration mode command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default configuration, use the `no` form of this command.

Syntax

```
spanning-tree mst instance-id cost cost
no spanning-tree mst instance-id cost
```

- `cost` — The port path cost. (Range: 1 - 200,000,000)

Default Setting

Default path cost is determined by port speed and path cost method (long or short) as shown below:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000 Mbps)</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Fast Ethernet (100 Mbps)</td>
<td>200,000</td>
<td>19</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Default Configuration

There is no default configuration for this command.

Example

The following example configures the MSTP instance 1 path cost for Ethernet port e9 to 4.

```
Console(config) # interface ethernet 1/e9
Console(config-if) # spanning-tree mst 1 cost 4
```

spanning-tree mst configuration

The `spanning-tree mst configuration` Global Configuration mode command enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.
Syntax

spanning-tree mst configuration

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- All devices in an MST region must have the same VLAN mapping, configuration revision number, and name.

Example

The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration
Console(config-mst) # instance 1 add vlan 10-20
Console(config-mst) # name region1
Console(config-mst) # revision 1
```

instance (mst)

The `instance` MST Configuration mode command maps VLANs to an MST instance.

Syntax

```
instance instance-id {add | remove} vlan vlan-range
```

- **instance-ID** — ID of the MST instance (Range: 1-8).
- **vlan-range** — VLANs to be added to or removed from the specified MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4094).

Default Setting

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

User Guidelines

- All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.
For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

**Example**
The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 add vlan 10-20
```

**name (mst)**
The `name` MST Configuration mode command defines the configuration name. To return to the default setting, use the `no` form of this command.

**Syntax**
```
name string
```
- `string`—MST configuration name. Case-sensitive (Range: 1-32 characters).

**Default Setting**
The default name is a bridge ID.

**Command Mode**
MST Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example defines the configuration name as regional.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# name region 1
```

**revision (mst)**
The `revision` MST configuration command defines the configuration revision number. To return to the default configuration, use the `no` form of this command.

**Syntax**
```
revision value
no revision
```
- `value` — Configuration revision number (Range: 0-65535).
Default Setting
The default configuration revision number is 0.

Command Mode
MST Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

show (mst)
The `show mst` Configuration mode command displays the current or pending MST region configuration.

Syntax
```
show {current | pending}
```
- `current` — Indicates the current region configuration.
- `pending` — Indicates the pending region configuration.

Default Setting
This command has no default configuration.

Command Mode
MST Configuration mode

User Guidelines
- The pending MST region configuration takes effect only after exiting the MST configuration mode.

Example
The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending
Pending MST configuration
```
exit (mst)

The `exit` MST Configuration mode command exits the MST configuration mode and applies all configuration changes.

**Syntax**

```
exit
```

**Default Setting**

This command has no default configuration.

**Command Mode**

MST Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example exits the MST configuration mode and saves changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # exit
```

abort (mst)

The `abort` MST Configuration mode command exits the MST configuration mode without applying the configuration changes.

**Syntax**

```
abort
```

**Default Setting**

This command has no default configuration.
Spanning-Tree Commands

Command Mode
MST Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example exits the MST configuration mode without saving changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # abort
```

spanning-tree pathcost method
The spanning-tree pathcost method Global Configuration mode command sets the default path cost method. To revert to the default setting, use the no form of this command.

Syntax
```
spanning-tree pathcost method {long | short}
no spanning-tree pathcost method
```

- **long**—Specifies 1 through 200,000,000 range for port path costs.
- **short**—Specifies 0 through 65,535 range for port path costs.

Default Configuration
Short

Command Mode
Global configuration mode

User Guidelines
- The cost is set using the spanning-tree cost command.

Example
The following example sets the default path cost method to "long".

```
Console# spanning-tree pathcost method long
```

spanning-tree bpdu
The spanning-tree bpdu Global Configuration mode command defines BPDUs handling when spanning-tree is disabled on an interface.
Syntax

```
spanning-tree bpdu {filtering | flooding}
```

- **filtering**—Filter BPDU packets when spanning-tree is disabled on an interface.
- **flooding**—Flood BPDU packets when spanning-tree is disabled on an interface.

**Default Configuration**

The default definition is flooding.

**Command Modes**

- Global Configuration mode

**User Guidelines**

- The command is relevant when spanning-tree is disabled globally or on a single interface.

**Example**

The following example defines BPDU packet flooding when spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdu flooding
```

**clear spanning-tree detected-protocols**

The clear spanning-tree detected-protocols Privileged EXEC mode command restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

**Syntax**

```
clear spanning-tree detected-protocols [ethernet interface number | port-channel port-channel-number]
```

- **interface**—A valid Ethernet port.
- **port-channel-number**—A port-channel index.

**Default Configuration**

If no interface is specified, the action is applied to all interfaces.

**Command Modes**

- Privileged EXEC mode

**User Guidelines**

- This feature should be used only when working in RSTP mode.
Example
The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on g1.

```
Console# clear spanning-tree detected-protocols ethernet g1
```

**show spanning-tree**
The `show spanning-tree` Privileged EXEC mode command displays spanning-tree configuration.

**Syntax**
```
show spanning-tree [ethernet interface-number | port-channel port-channel-number] [instance instance-id]
show spanning-tree [detail] [active | blockedports] [instance instance-id]
show spanning-tree mst-configuration
  - detail — Display detailed information.
  - active — Display active ports only.
  - blockedports — Display blocked ports only.
  - mst-configuration — Display the MST configuration identifier.
  - interface-number — Ethernet port number. (Range:Valid Ethernet port)
  - port-channel-number — Port channel index. (Range:Valid Ethernet port)
  - instance-id — ID associated with a spanning-tree instance.
```

**Default Configuration**
This command has no default configuration.

**Command Modes**
Privileged EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

**Examples**
The following example displays spanning-tree information.
Console# `show spanning-tree`

Spanning tree enabled mode RSTP  
Default port cost method: long

Root ID    Priority 32768  
Address 00:01:42:97:e0:00  
Path Cost 2000  
Root Port 1(1/1)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority 36864  
Address 00:02:4b:29:7a:00  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
console# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Shared (STP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Shared (STP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This switch is the Root.
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>128.1</td>
<td></td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>2</td>
<td>Enabled</td>
<td>128.2</td>
<td></td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>3</td>
<td>Disabled</td>
<td>128.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Enabled</td>
<td>128.4</td>
<td></td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>5</td>
<td>Enabled</td>
<td>128.5</td>
<td></td>
<td>DIS</td>
<td></td>
<td>20000</td>
<td></td>
</tr>
</tbody>
</table>

Console# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Spanning-Tree Commands

```
Path Cost      N/A
Root Port      N/A
Hello Time N/A  Max Age N/A  Forward Delay N/A

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>36864</td>
<td>00:02:4b:29:7a:00</td>
</tr>
</tbody>
</table>

Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Console# show spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:01:42:97:e0:00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 (1/1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec</td>
</tr>
</tbody>
</table>

| Bridge ID | Priority | 36864 |
```

---

Spanning-Tree Commands  |  281
Answer:Spanning-Tree Commands

Address 00:02:4b:29:7a:00

Hello Time 2 sec  Max Age 20 sec  Forward
Delay 15 sec

Interfaces
Name State Prio.Nbr Cost Sts Role PortFast Type
1/1 Enabled 128.1 20000 FWD Root No P2p (RSTP)
1/2 Enabled 128.2 20000 FWD Desg No Shared (STP)
1/4 Enabled 128.4 20000 BLK Altn No Shared (STP)

console# show spanning-tree blockedports

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID Priority 32768
Address 00:01:42:97:e0:00
Path Cost 20000
Root Port 1 (1/1)
Hello Time 2 sec  Max Age 20 sec  Forward
Delay 15 sec

Bridge ID Priority 36864
Address       00:02:4b:29:7a:00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces
Name       State     Prio.Nbr   Cost  Sts  Role  PortFast  Type
1/4        Enabled  128.4      19    BLK  Altn  No

Console# show spanning-tree detail

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID     Priority  32768
            Address   00:01:42:97:e0:00
            Path Cost  20000
            Root Port  1 (1/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID   Priority  36864
            Address   00:02:4b:29:7a:00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 2d18h ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15

State: Forwarding          Role: Root
<table>
<thead>
<tr>
<th>Port id: 128.1</th>
<th>Port cost: 20000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: P2p (configured: auto) RSTP</td>
<td>Port Fast: No (configured:no)</td>
</tr>
<tr>
<td>Designated bridge Priority: 32768</td>
<td>Address: 00:01:42:97:e0:00</td>
</tr>
<tr>
<td>Designated port id: 128.25</td>
<td>Designated path cost: 0</td>
</tr>
<tr>
<td>Guard root: Disabled</td>
<td>BPDU guard: Disabled</td>
</tr>
<tr>
<td>Number of transitions to forwarding state: 1</td>
<td></td>
</tr>
<tr>
<td>BPDU: sent 2, received 120638</td>
<td></td>
</tr>
</tbody>
</table>

Port 2 (1/2) enabled
<table>
<thead>
<tr>
<th>State: Forwarding</th>
<th>Role: Designated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port id: 128.2</td>
<td>Port cost: 20000</td>
</tr>
<tr>
<td>Type: Share d (configured: auto) STP</td>
<td>Port Fast: No (configured:no)</td>
</tr>
<tr>
<td>Designated bridge Priority: 32768</td>
<td>Address: 00:02:4b:29:7a:00</td>
</tr>
<tr>
<td>Designated port id: 128.2</td>
<td>Designated path cost: 20000</td>
</tr>
<tr>
<td>Guard root: Disabled</td>
<td>BPDU guard: Disabled</td>
</tr>
<tr>
<td>Number of transitions to forwarding state: 1</td>
<td></td>
</tr>
<tr>
<td>BPDU: sent 2, received 170638</td>
<td></td>
</tr>
</tbody>
</table>

Port 3 (1/3) disabled
<table>
<thead>
<tr>
<th>State: N/A</th>
<th>Role: N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port id: 128.3</td>
<td>Port cost: 20000</td>
</tr>
<tr>
<td>Type: N/A (configured: auto)</td>
<td>Port Fast: N/A (configured:no)</td>
</tr>
<tr>
<td>Designated bridge Priority: N/A</td>
<td>Address: N/A</td>
</tr>
<tr>
<td>Designated port id: N/A</td>
<td>Designated path cost: N/A</td>
</tr>
<tr>
<td>Guard root: Disabled</td>
<td>BPDU guard: Disabled</td>
</tr>
<tr>
<td>Number of transitions to forwarding state: N/A</td>
<td></td>
</tr>
<tr>
<td>BPDU: sent N/A, received N/A</td>
<td></td>
</tr>
</tbody>
</table>
Port 4 (1/4) enabled
State: Blocking   Role: Alternate
Port Identifier: 128.4   Port cost: 20000
Type: Shared (configured: auto) STP   Port Fast: No (configured:no)
Designated bridge Priority: 28672   Address: 00:30:94:41:62:c8
Designated port id: 128.25   Designated path cost: 20000
Guard root: Disabled   BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDUs: sent 2, received 120638

Port 5 (1/5) enabled
State: Disabled   Role: N/A
Port id: 128.5   Port cost: 20000
Type: N/A (configured: auto)   Port Fast: N/A (configured:no)
Designated bridge Priority: N/A   Address: N/A
Designated port id: N/A   Designated path cost: N/A
Guard root: Disabled   BPDU guard: Disabled
Number of transitions to forwarding state: N/A
BPDUs: sent N/A, received N/A

Console# show spanning-tree ethernet 1/1
Port 1 (1/1) enabled
State: Forwarding   Role: Root
Port id: 128.1   Port cost: 20000
Type: P2p (configured: auto) RSTP   Port Fast: No (configured:no)
Designated bridge Priority: 32768   Address: 00:01:42:97:e0:00
Designated port id: 128.25  Designated path cost: 0
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Console# show spanning-tree mst-configuration

Name: Region1
Revision: 1

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans Mapped</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-9, 21-4094</td>
<td>Enabled</td>
</tr>
<tr>
<td>1</td>
<td>10-20</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Console# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:01:42:97:e0:00</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>20000</td>
<td></td>
</tr>
<tr>
<td>Root Port</td>
<td>1 (1/1)</td>
<td></td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td>Max Age 20 sec  Forward Delay 15 sec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:29:7a:00</td>
<td></td>
</tr>
</tbody>
</table>
Hello Time 2 sec This switch is the IST master. Max Age 20 sec Forward Delay 15 sec Max hops 20

### MST 1 Vlans Mapped: 10-20

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>24576</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:29:89:76</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>20000</td>
<td></td>
</tr>
<tr>
<td>Root Port</td>
<td>4(1/4)</td>
<td></td>
</tr>
<tr>
<td>Rem hops</td>
<td>19</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:29:7a:00</td>
<td></td>
</tr>
</tbody>
</table>

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Number</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>128.1</td>
<td>FWD</td>
<td>No</td>
<td>P2p</td>
<td>Bound</td>
<td>(RSTP)</td>
</tr>
<tr>
<td>2</td>
<td>Enabled</td>
<td>128.2</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared</td>
<td>Bound</td>
</tr>
<tr>
<td>3</td>
<td>Enabled</td>
<td>128.3</td>
<td>FWD</td>
<td>No</td>
<td>P2p</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Enabled</td>
<td>128.4</td>
<td>FWD</td>
<td>No</td>
<td>P2p</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Number of topology changes 2 last change occurred 1d9h ago
Times:  hold 1, topology change 2, notification 2
hello 2, max age 20, forward delay 15

Port 1 (1/1) enabled
State: Forwarding  Role: Boundary
Port id: 128.1  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.1  Designated path cost: 20000
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (1/2) enabled
State: Forwarding  Role: Designated
Port id: 128.2  Port cost: 20000
Type: Shared (configured: auto) Boundary STP  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Guard root: Disabled  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (1/3) disabled
State: Blocking  Role: Alternate
Port id: 128.3  Port cost: 20000
Type: Shared (configured: auto) Internal  Port Fast: No (configured:no)
Designated bridge Priority: 32768  Address: 00:02:4b:29:1a:19
Designated port id: 128.78  Designated path cost: 20000
Spanning-Tree Commands

Guard root: Disabled          BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
Port 4 (1/4) enabled
State: Forwarding            Role: Designated
  Port id: 128.4               Port cost: 20000
  Type: Shared (configured: auto) Internal
  Designated bridge Priority: 32768
  Designated port id: 128.2
  Guard root: Disabled
  BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

#### MST 0 Vlans Mapped: 1-9

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:01:42:97:e0:00</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>20000</td>
<td></td>
</tr>
<tr>
<td>Root Port</td>
<td>1 (1/1)</td>
<td></td>
</tr>
<tr>
<td>Hello Time</td>
<td>2 sec</td>
<td></td>
</tr>
<tr>
<td>Max Age</td>
<td>20 sec</td>
<td></td>
</tr>
<tr>
<td>Forward Delay</td>
<td>15 sec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
</table>
spanning-tree mst mstp-rstp

Use the `spanning-tree mst mstp-rstp` global configuration command to configure the switch to convert STP/RSTP packets to MSTP instances. Use the `no` form of this command to disable the configuration.

**Syntax**

```plaintext
spanning-tree mst mstp-rstp
no spanning-tree mst mstp-rstp
```

This command has no arguments or keywords.
Default Configuration
Disabled.

Command Modes
Global configuration

User Guidelines
- This command can be enabled when all the ports are Access ports.
- This command is relevant in MSTP mode only.
- When this feature is enabled incoming IEEE RSTP/STP packets would be mapped to the MSTP instance according to the port’s VLAN. Outgoing MSTP packets would be mapped to IEEE RSTP/STP packets according to the port’s VLAN.

Example
The following example configures the switch to convert STP/RSTP packets to MSTP instances.

```
Console(config)# spanning-tree mst mstp-rstp
```

Spanning-tree guard root
Use the `spanning-tree guard root` interface configuration command to enable root guard on all the spanning tree instances on that interface. Root guard restricts the interface to be the root port for the switch. Use the no form of this command to disable root guard on the interface.

Syntax
```
spanning-tree guard root
no spanning-tree guard root
```

Default Configuration
Root guard is disabled

Command Modes
Interface configuration (Ethernet, port-channel)

User Guidelines
- Root guard can be enabled when the switch work in STP, RSTP and MSTP.
- When root guard is enabled, if spanning-tree calculations cause a port to be selected as the root port, the port transitions to the alternate state.
**Example**

The following example enable root guard on port g8.

```
Console(config)# interface ethernet g8
Console(config-if)# spanning-tree guard root
```
SSH Commands

**ip ssh port**
The `ip ssh port` Global Configuration mode command specifies the port to be used by the SSH server. To use the default port, use the `no` form of this command.

**Syntax**
```
ip ssh port port-number
no ip ssh port
```
* `port-number`—Port number for use by the SSH server (Range: 1 - 65535).

**Default Configuration**
The default value is 22.

**Command Mode**
Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example specifies the port to be used by the SSH server as 8080.

```
Console (config)# ip ssh port 8080
```

**ip ssh server**
The `ip ssh server` Global Configuration mode command enables the device to be configured from a SSH server. To disable this function, use the `no` form of this command.

**Syntax**
```
ip ssh server
no ip ssh server
```

**Default Configuration**
SSH is enabled.

**Command Mode**
Global Configuration mode
User Guidelines

- If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the commands `crypto key generate rsa`, and `crypto key generate dsa`.

Example

The following example enables the device to be configured from a SSH server.

```
Console (config)# ip ssh server
```

**crypto key generate dsa**

The `ip ssh server` Global Configuration mode command generates DSA key pairs.

**Syntax**

```
crypto key generate dsa
```

**Default Configuration**

DSA key pairs do not exist.

**Command Mode**

Global Configuration mode

**User Guidelines**

- DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys is displayed.
- This command is not saved in the startup configuration; however, the keys generated by this command are saved in the FLASH. The SSH keys can be displayed with the `show crypto key mypubkey dsa` command.
- This command may take a considerable period of time to execute.
- DSA key size is 2048 bits.

**Example**

The following example generates DSA key pairs.

```
Console (config)# crypto key generate dsa
```

**crypto key generate rsa**

The `crypto key generate rsa` Global Configuration mode command generates RSA key pairs.
Syntax

crypto key generate rsa

Default Configuration
RSA key pairs do not exist.

Command Mode
Global Configuration mode

User Guidelines
- RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys is displayed.
- The maximum supported size for the RSA key is 2048 bits.
- This command is not saved in the startup configuration; however, the keys generated by this command are saved in the FLASH. The SSH keys can be displayed with the show crypto key mypubkey rsa command.
- This command may take a considerable period of time to execute.

Example
The following example generates RSA key pairs.

```
Console (config)# crypto key generate rsa
```

**ip ssh pubkey-auth**
The `ip ssh pubkey-auth` Global Configuration mode command enables public key authentication for incoming SSH sessions. To disable this function, use the `no` form of this command.

Syntax

```
ip ssh pubkey-auth
  no ip ssh pubkey-auth
```

Default Configuration
The function is disabled.

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.
Example
The following example enables public key authentication for incoming SSH sessions.

```
Console (config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh
The `crypto key pubkey-chain ssh` Global Configuration mode command enters SSH Public Key-chain configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

Syntax
```
crypto key pubkey-chain ssh
```

Default Configuration
By default, there are no keys.

Command Mode
Global Configuration mode

User Guidelines
- Use this command to enter public key chain configuration mode.
- This command can also be used when you need to manually specify SSH client’s public keys.

Example
The following example enters the SSH Public Key-chain configuration mode.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)#
```

user-key
The `user-key` SSH Public Key Chain Configuration mode command specifies which SSH public key is manually configured and enters the SSH public key-string configuration command. To remove a SSH public key, use the `no` form of this command.

Syntax
```
user-key username {rsa | dsa}
no user-key username
```

- `username`—Specifies the remote SSH client username, which can be up to 48 characters long.
- `rsa`—RSA key.
• dsa—DSA key.

Default Configuration
By default, there are no keys.

Command Mode
SSH Public Key Chain Configuration mode

User Guidelines
• Follow this command with the key-string command to specify the key.

Example
The following example enables a SSH public key to be manually configured for the SSH public key chain called "bob".

```
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWL
```

key-string
The key-string SSH Public Key-String Configuration mode command manually specifies a SSH public key.

Syntax
key-string row key-string

  • row—Specify SSH public key row by row
  • key-string—UU-encoded DER format is the same format in authorized_keys file used by OpenSSH.

Default Configuration
By default, the keys do not exist.

Command Mode
SSH Public Key-string configuration

User Guidelines
• Use the key-string row command to specify the SSH public key row by row. Each row must begin with the key-string row command. This command is useful for configuration files.
• UU-encoded DER format is the same format in authorized_keys file used by OpenSSH.
Example
The following example enters public key strings for SSH public key clients called "bob".

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQ0TgVR4AQK6rjXgX069w1+
A14k9QIw9GBR0nZQxjHKqKL6rMLQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSw0QvV35LqJk67IOU/zfw01lg
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQw081icglk02LYciz
+z4TrEU/9FJxwP1VQ0jc+KBXuR0juNg5nFYSY
0ZCk0N/W9a/tnkm1shRE7D171+w3fNiOA
6w9o44t6+AINEICBCC4YcF6zMzaTlwefWwX6f+
Rmt5nhqtdtN/4oJfcej66DqVX1gWmN
zNR4DYDvSzg01DnwCAC8Qh
```


**show ip ssh**
The `show ip ssh` Privileged EXEC mode command displays the SSH server configuration.

**Syntax**
```
show ip ssh
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- There are no user guidelines for this command.
Example
The following example displays the SSH server configuration.

```
Console# show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:

<table>
<thead>
<tr>
<th>IP address</th>
<th>SSH username</th>
<th>Version</th>
<th>Cipher</th>
<th>Auth Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.1</td>
<td>John Brown</td>
<td>2.0</td>
<td>DES</td>
<td>HMAC-SH1</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Client address</td>
</tr>
<tr>
<td>SSH username</td>
<td>User name</td>
</tr>
<tr>
<td>Version</td>
<td>SSH version number</td>
</tr>
<tr>
<td>Cipher</td>
<td>Encryption type (3DES, Blowfish, RC4)</td>
</tr>
<tr>
<td>Auth Code</td>
<td>Authentication Code (HMAC-MD5, HMAC-SHA1)</td>
</tr>
</tbody>
</table>

```
show crypto key mypubkey
```

The `show crypto key mypubkey` Privileged EXEC mode command displays the SSH public keys on the device.

**Syntax**

```
show crypto key mypubkey [rsa | dsa]
```

- rsa—RSA key.
- dsa—DSA key.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode
User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the SSH public keys on the device.

```
Console# show crypto key mypubkey rsa
RSA key data:
005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 87685768
Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt gfhkjglk
```

**show crypto key pubkey-chain ssh**

The `show crypto key pubkey-chain ssh` Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

```
show crypto key pubkey-chain ssh [username username] [fingerprint bubble-babble | hex]
```

- **username**—Specifies the remote SSH client username.
- **bubble-babble**—Fingerprints in Bubble Babble format.
- **hex**—Fingerprint in Hex format. If fingerprint is unspecified, it defaults to Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- There are no user guidelines for this command.

Examples

The following example displays all SSH public keys stored on the device.
The following example displays the SSH public called "bob".

```console
Console# show crypto key pubkey-chain ssh
Username    Fingerprint
----------  -----------------------------------------------
```

```console
Console# show crypto key pubkey-chain ssh username bob
Username: bob
Key: 005C300D 06092A86
```
Syslog Commands

logging on
The `logging on` Global Configuration mode command controls error messages logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the `no` form of this command.

**Syntax**
```
logging on
no logging on
```

**Default Configuration**
Logging is enabled.

**Command Mode**
Global Configuration mode

**User Guidelines**
- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. Logging on and off for these destinations can be individually configured using the `logging buffered`, `logging file`, and `logging` Global Configuration mode commands. However, if the `logging on` command is disabled, no messages are sent to these destinations. Only the console receives messages.

**Example**
The following example shows how logging is enabled.

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

**logging**
The `logging` Global Configuration mode command logs messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the `no` form of this command.

**Syntax**
```
logging {ip-address | hostname} [port port] [severity level] [facility facility] [description text]
no logging {ip-address | hostname}
```
- `ip-address`—IP address of the host to be used as a syslog server.
- `hostname`—Hostname of the host to be used as a syslog server. (Range: 1 - 158 characters)
- **port**—Port number for syslog messages. If unspecified, the port number defaults to 514. (Range: 1 - 65535)
- **severity level**—Limits the logging of messages to the syslog servers to a specified level: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging. If unspecified, the default level is errors.
- **facility**—The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local6, local7. If unspecified, the port number defaults to local7.
- **text**—Syslog server description, which can be up to 64 characters.

**Default Configuration**
As described in the field descriptions.

**Command Mode**
Global Configuration mode

**User Guidelines**
- Multiple syslog servers can be used.
- If no specific severity level is specified, the global values apply to each server.

**Example**
The following example configures messages with a "critical" severity level so that they are logged to a syslog server with an IP address 10.1.1.1.

```
Console (config)# logging 10.1.1.1 severity critical
```

**logging console**
The **logging console** Global Configuration mode command limits messages logged to the console based on severity. To disable logging to the console terminal, use the **no** form of this command.

**Syntax**
logging console level

no logging console

- **level**—Limits the logging of messages displayed on the console to a specified level: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.

**Default Configuration**
The default is informational.
**Command Mode**

- Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example limits messages logged to the console based on severity level "errors".

```
Console (config)# logging console errors
```

**logging buffered**

The **logging buffered** Global Configuration mode command limits syslog messages displayed from an internal buffer based on severity. To cancel the buffer use, use the **no** form of this command.

**Syntax**

```
logging buffered level
no logging buffered
```

- **level**—Limits the message logging to a specified level buffer: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.

**Default Configuration**

The default level is **informational**.

**Command Mode**

- Global Configuration mode

**User Guidelines**

- All the syslog messages are logged to the internal buffer. This command limits the commands displayed to the user.

**Example**

The following example limits syslog messages displayed from an internal buffer based on the severity level "debugging".

```
Console (config)# logging buffered debugging
```

**logging buffered size**

The **logging buffered size** Global Configuration mode command changes the number of syslog messages stored in the internal buffer. To return the number of messages stored in the internal buffer to the default value, use the **no** form of this command.
Syslog Commands

Syntax

logging buffered size number

no logging buffered size

- number—Numeric value indicating the maximum number of messages stored in the history table. (Range: 20 - 400)

Default Configuration

The default number of messages is 200.

Command Mode

Global Configuration mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console (config)# logging buffered size 300

```

clear logging

The clear logging Privileged EXEC mode command clears messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example clears messages from the internal syslog message logging buffer.

```
Console# clear logging
Clear logging buffer [y/n] y
```
logging file

The *logging file* Global Configuration mode command limits syslog messages sent to the logging file based on severity. To cancel the buffer, use the no form of this command.

**Syntax**

```
logging file level
no logging file
```

- *level*—Limits the logging of messages to the buffer to a specified level: *emergencies*, *alerts*, *critical*, *errors*, *warnings*, *notifications*, *informational* and *debugging*.

**Default Configuration**

The default severity level is *errors*.

**Command Mode**

Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example limits syslog messages sent to the logging file based on the severity level "alerts".

```
Console (config)# logging file alerts
```

clear logging file

The *clear logging file* Privileged EXEC mode command clears messages from the logging file.

**Syntax**

```
clear logging file
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.
Example
The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [y/n]y
```

show logging
The show logging Privileged EXEC mode command displays the state of logging and the syslog messages stored in the internal buffer.

Syntax
```
show logging
```

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.
Example
The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
Console# show logging
Logging is enabled.
Buffer Logging: Level debug. Buffer Messages: 16 Logged, 16 Displayed, 200 Max.
SysLog server 5.2.2.2 Logging: info. Messages: 0 Dropped.
SysLog server 10.2.2.2 Logging: critical. Messages: 21 Dropped.
1 messages were not logged

03-Mar-2004 12:02:03 :%LINK-I-Up:  g1
03-Mar-2004 12:02:01 :%LINK-W-Down:  g2
03-Mar-2004 12:02:01 :%LINK-I-Up:  g3
```

**show logging file**
The `show logging file` Privileged EXEC mode command displays the state of logging and the syslog messages stored in the logging file.

**Syntax**
```text
show logging file
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode
User Guidelines

- There are no user guidelines for this command.

Example

The following example displays the state of logging and the syslog messages stored in the logging file.

```
Console # show logging file
console# show logging file
Logging is enabled.
SysLog server 5.2.2.2 Logging: info. Messages: 0 Dropped.
SysLog server 10.2.2.2 Logging: critical. Messages: 26 Dropped.
1 messages were not logged

03-Mar-2004 12:04:08 :%LINK-I-Up: g1
03-Mar-2004 12:04:06 :%LINK-W-Down: g2
03-Mar-2004 12:04:06 :%LINK-I-Up: g3
03-Mar-2004 12:04:04 :%LINK-W-Down: g4
```

**show syslog-servers**

The show syslog-servers Privileged EXEC mode command displays the syslog servers settings.

**Syntax**

```
show syslog-servers
```

**Default Configuration**

- This command has no default configuration.
**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the syslog server settings.

```
Console# show syslog-servers

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>Severity</th>
<th>Facility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.180.2.275</td>
<td>14</td>
<td>Informational</td>
<td>local</td>
<td>7</td>
</tr>
<tr>
<td>192.180.2.285</td>
<td>14</td>
<td>Warning</td>
<td>local</td>
<td>7</td>
</tr>
</tbody>
</table>
```
System Management

ping
The ping User EXEC mode command sends ICMP echo request packets to another node on the network.

Syntax
```
ping ip-address | hostname [size packet_size] [count packet_count] [timeout time_out]
```
- `ip-address`—IP address to ping.
- `hostname`—Hostname to ping. (Range: 1 - 158 characters)
- `packet_size`—Number of bytes in a packet. The actual packet size is eight bytes larger than the size specified because the switch adds header information. (Range: 56 - 1472 bytes)
- `packet_count`—Number of packets to send. If 0 is entered it pings until stopped. (Range: 0 - 65535 packets)
- `time_out`—Timeout in milliseconds to wait for each reply. (Range: 50 - 65535 milliseconds).

Default Configuration
```
timeout time_out—The default is 2000 milliseconds.
```

Command Mode
```
User EXEC mode
```

User Guidelines
```
Press Esc to stop pinging. Following are sample results of the ping command:
- Destination (host/network) unreachable—The gateway for this destination indicates that the destination is unreachable.
```

```
Console# ping 180.50.1.1
Pinging 180.50.1.1 with 56 bytes of data:
PING: net-unreachable
PING: net-unreachable
PING: net-unreachable
```

Examples
The following example displays a ping to IP address 10.1.1.1.

```
Console> ping 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

**traceroute**
The **traceroute** User EXEC mode command discovers the routes that packets will actually take when traveling to their destination.

**Syntax**
```
traceroute ip-address | hostname [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
```
- **ip-address**—IP address of the destination host. (Range: Valid IP Address)
- **hostname**—Hostname of the destination host (Range: 1 - 158 characters)
- **size packet_size**—Number of bytes in a packet. (Range: 40-1472)
- **ttl max-ttl**—The largest TTL value that can be used. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range:1-255)
- **count packet_count**—The number of probes to be sent at each TTL level. (Range:1-10)
- **timeout time_out**—The number of seconds to wait for a response to a probe packet. (Range:1-60)
• **source ip-address**—One of the interface addresses of the device to use as a source address for the probes. The device will normally pick what it feels is the best source address to use. (Range: Valid IP Address)

• **tos**—The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

**Default Configuration**

- **size packet_size**—The default is 40 bytes.
- **ttl max-ttl**—The default is 30.
- **count packet_count**—The default count is 3.
- **timeout time_out**—The default is 6 seconds.

**Command Mode**

User EXEC mode

**User Guidelines**

- The `traceroute` command works by taking advantage of the error messages generated by a device when a datagram exceeds its time-to-live (TTL) value.
- The `traceroute` command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The `traceroute` command sends several probes at each TTL level and displays the round-trip time for each.
- The `traceroute` command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate device has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the `traceroute` command prints an asterisk (*).
- The `traceroute` command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with **Esc**.
Examples

console> traceroute umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83) 0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162) 1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 33 msec 35 msec 35 msec
6 iplnsg-kscyng.abilene.ucaid.edu (198.32.8.80) 47 msec 45 msec 45 msec
7 so-0-2-0x1.aal1.mich.net (192.122.183.9) 56 msec 53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82) 56 msec 56 msec 56 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58 msec 58 msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64) 62 msec 63 msec 63 msec

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates the sequence number of the router in the path to the host.</td>
</tr>
<tr>
<td>i2-gateway.stanford.edu</td>
<td>Host name of this device.</td>
</tr>
<tr>
<td>192.68.191.83</td>
<td>IP address of this device.</td>
</tr>
<tr>
<td>1 msec 1 msec 1 msec</td>
<td>Round-trip time for each of the probes that are sent.</td>
</tr>
</tbody>
</table>

The following table describes the characters that can appear in the `traceroute` command output.
The `telnet` User EXEC mode command is used to log in to a host that supports Telnet.

**Syntax**

```
telnet {ip-address | hostname} [port] [keyword1......]
```

- `ip-address`—IP address of the destination host. (Range: 1 - 160 characters)
- `hostname`—Hostname of the destination host (Range: Valid IP Address)
- `port`—A decimal TCP port number, or one of the keywords from the ports table in the usage guidelines. The default is the Telnet port (decimal23) on the host.
- `keyword`—Can be one or more keywords from the keywords table in the User Guidelines.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode

**User Guidelines**

- The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter Esc and then a command character.

**Special Telnet Command characters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>
At any time during an active Telnet session, the Telnet commands can be listed by pressing the Ctrl-shift-6 key, followed by a question mark at the system prompt: Ctrl-shift-6?

A sample of this list follows.

```
Console> 'Ctrl-shift-6' ?
[Special telnet escape help]
Esc B sends telnet BREAK
Esc C sends telnet IP
Esc H sends telnet EC
Esc O sends telnet AO
Esc T sends telnet AYT
Esc U sends telnet EL
Esc x suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened and switched between them. To open a subsequent session, the current connection needs to be suspended, by pressing the escape sequence ‘Ctrl-Shift-6’ and ‘x’ to return to the system command prompt. Then open a new connection with the telnet command.

### Keywords Table

<table>
<thead>
<tr>
<th>Escape Sequence</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-shift-6 b</td>
<td>Break</td>
</tr>
<tr>
<td>Ctrl-shift-6 c</td>
<td>Interrupt Process (IP)</td>
</tr>
<tr>
<td>Ctrl-shift-6 h</td>
<td>Erase Character (EC)</td>
</tr>
<tr>
<td>Ctrl-shift-6 o</td>
<td>Abort Output (AO)</td>
</tr>
<tr>
<td>Ctrl-shift-6 t</td>
<td>Are You There? (AYT)</td>
</tr>
<tr>
<td>Ctrl-shift-6 u</td>
<td>Erase Line (EL)</td>
</tr>
<tr>
<td>Ctrl-shift-6 x</td>
<td>Suspends the Session</td>
</tr>
</tbody>
</table>

The following options can be added to the telnet command.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/echo</td>
<td>Enables local echo</td>
</tr>
<tr>
<td>/quiet</td>
<td>Prevents onscreen display of all messages from the software.</td>
</tr>
<tr>
<td>/source-interface</td>
<td>Specifies the source interface.</td>
</tr>
</tbody>
</table>
Ports Table

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Border Gateway Protocol</td>
<td>179</td>
</tr>
<tr>
<td>chargen</td>
<td>Character generator</td>
<td>19</td>
</tr>
<tr>
<td>cmd</td>
<td>Remote commands</td>
<td>514</td>
</tr>
<tr>
<td>daytime</td>
<td>Daytime</td>
<td>13</td>
</tr>
<tr>
<td>discard</td>
<td>Discard</td>
<td>9</td>
</tr>
<tr>
<td>domain</td>
<td>Domain Name Service</td>
<td>55</td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
<td>7</td>
</tr>
<tr>
<td>exec</td>
<td>Exec</td>
<td>512</td>
</tr>
<tr>
<td>finger</td>
<td>Finger</td>
<td>79</td>
</tr>
<tr>
<td>ftp</td>
<td>File Transfer Protocol</td>
<td>21</td>
</tr>
<tr>
<td>ftp-data</td>
<td>FTP data connections</td>
<td>20</td>
</tr>
<tr>
<td>gopher</td>
<td>Gopher</td>
<td>70</td>
</tr>
<tr>
<td>hostname</td>
<td>NIC hostname server</td>
<td>101</td>
</tr>
<tr>
<td>ident</td>
<td>Ident Protocol</td>
<td>113</td>
</tr>
<tr>
<td>irc</td>
<td>Internet Relay Chat</td>
<td>194</td>
</tr>
<tr>
<td>klogin</td>
<td>Kerberos login</td>
<td>543</td>
</tr>
<tr>
<td>kshell</td>
<td>Kerberos shell</td>
<td>544</td>
</tr>
<tr>
<td>login</td>
<td>Login</td>
<td>513</td>
</tr>
<tr>
<td>lpd</td>
<td>Printer service</td>
<td>515</td>
</tr>
<tr>
<td>nntp</td>
<td>Network News Transport Protocol</td>
<td>119</td>
</tr>
<tr>
<td>pim-auto-rp</td>
<td>PIM Auto-RP</td>
<td>496</td>
</tr>
<tr>
<td>pop2</td>
<td>Post Office Protocol v2</td>
<td>109</td>
</tr>
</tbody>
</table>
resume
The `resume` User EXEC mode command is used to switch to another open Telnet session.

**Syntax**
```
resume [connection]
```
- `connection`—The connection number. The default is the most recent connection

**Default Configuration**
There is no default configuration for this command.

**Command Mode**
User EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

**Examples**
The following command switches to another open Telnet session.

```
Console> resume 176.213.10.50
```
**reload**
The `reload` Privileged EXEC mode command reloads the operating system.

**Syntax**
```
reload
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- Caution should be exercised when resetting the device, to ensure that no other activity is being performed. In particular, the user should verify that no configuration files are being downloaded at the time of reset.

**Example**
The following example reloads the operating system.
```
Console# reload
```

**hostname**
The `hostname` Global Configuration mode command specifies or modifies the device host name. To remove the existing host name, use the `no` form of the command.

**Syntax**
```
hostname name
no hostname
```

**name**—The device host name. Range (1-158 characters)

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.
Example
The following example specifies the device host name.

```
Console (config)# hostname Dell
```

**show users**
The `show users` User EXEC mode command displays information about the active users.

**Syntax**

```
show users
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
User EXEC mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example displays information about the active users.

```
Console# show users

<table>
<thead>
<tr>
<th>Username</th>
<th>Protocol</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>Serial</td>
<td></td>
</tr>
<tr>
<td>John</td>
<td>SSH</td>
<td>172.16.0.1</td>
</tr>
<tr>
<td>Robert</td>
<td>HTTP</td>
<td>172.16.0.8</td>
</tr>
</tbody>
</table>
```

**show sessions**
The `show sessions` User EXEC mode command lists the open Telnet sessions.

**Syntax**

```
show sessions
```

This command has no arguments or keywords.
Default Configuration
There is no default configuration for this command.

Command Mode
EXEC mode

User Guidelines
1  Open telnet session from PC 5324 to other device.
2  In the other device syntax, press Ctrl-shift-t-X
3  Enter the command show session. The number of sessions opened from PC 5324 is displayed.
4  Enter the command resume [number of session] to return to the relevant telnet session.

Examples
The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Host</th>
<th>Address</th>
<th>Port</th>
<th>Byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote device</td>
<td>172.16.1.1</td>
<td>23</td>
<td>89</td>
</tr>
<tr>
<td>2</td>
<td>172.16.1.2</td>
<td>172.16.1.2</td>
<td>23</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>Connection number</td>
</tr>
<tr>
<td>Host</td>
<td>Remote host to which the device is connected through a Telnet session.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the remote host.</td>
</tr>
<tr>
<td>Port</td>
<td>Telnet TCP port number</td>
</tr>
<tr>
<td>Byte</td>
<td>Number of unread bytes for the user to see on the connection.</td>
</tr>
</tbody>
</table>

show system
The show system User EXEC mode command displays system information.

Syntax
show system
**Default Configuration**
This command has no default configuration.

**Command Mode**
User EXEC mode

**User Guidelines**
There are no user guidelines for this command.

**Example**
The following example displays the system information.

```
console> show system
System Description: Corporate  
System Up Time (days, hour:minute:second): 1,22:38:21  
System Contact:  
System Name: RS1  
System location:  
System MAC Address: 00:10:B5:F4:00:01  
Sys Object ID:  
Type: PowerConnect 5324

Power Supply Status
------------- ---------------------
Main OK  
Secondary OK  

Fan Status
----------- ---------------------
1 OK  
2 OK
```

**show version**
The `show version` User EXEC mode command displays the system version information.

**Syntax**
```
show version
```
Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

• There are no user guidelines for this command.

Example

The following example displays a system version (this version number is only for demonstration purposes).

Router# show version
SW version 3.131 ( date 23-Jul-2002 time 17:34:19 )
HW version 1.0.0

Router# show clock
15:29:03 Jun 17 2002

Router# show history
show version
show clock
show history
3 commands were logged (buffer size is 10)

asset-tag

The asset-tag Global Configuration mode command specifies the device asset tag. To remove the existing asset tag, use the no form of the command.

Syntax

asset-tag tag
no asset-tag

• tag—The device asset tag. (Range: 1-16 characters)
**Default Configuration**

This command has no default configuration. No asset tag is defined by default.

**Command Mode**

- Global Configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example specifies the device asset tag as "1qwepot".

```
Console (config)# asset-tag 1qwepot
```

**show system id**

The `show system id` User EXEC mode command displays the ID information.

**Syntax**

```
show system id
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

- User EXEC mode

**User Guidelines**

- The tag information is on a device by device basis.

**Example**

The following example displays the system service tag information.

```
Console> show system id
Service Tag: 89788978
Serial number: 8936589782
Asset tag: 7843678957
```
TACACS Commands

tacacs-server host

The tacacs-server host Global Configuration mode command specifies a TACACS+ host. To delete the specified name or address, use the no form of this command.

Syntax

```
tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]
```

```
no tacacs-server host {ip-address | hostname}
```

- **ip-address**—Name or IP address of the host.
- **hostname**—Hostname of the tacacs server. (Range: 1 - 158 characters)
- **single-connection**—Specify single-connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the device and the daemon.
- **port-number**—Specify a server port number. If unspecified, the port number defaults to 49. (Range: 0 - 65535)
- **timeout**—Specifies the timeout value in seconds. If no timeout value is specified, the global value is used. (Range: 1 - 30)
- **key-string**—Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the encryption used on the TACACS daemon. If no key string value is specified, the global value is used. (Range: 0 - 128 characters)
- **source**—Specifies the source IP address to use for the communication. If no source value is specified, the global value is used.
- **priority**—Determines the order in which the servers will be used, when 0 is the highest priority. If unspecified defaults to 0. (Range: 0 - 65535)

Default Configuration

No TACACS host is specified

Command Mode

Global Configuration mode

User Guidelines

- Multiple tacacs-server host commands can be used to specify multiple hosts.
If no host-specific timeout, key or source values are specified, the global values apply to each host.

**Example**
The following example specifies a TACACS+ host.

```
Console (config)# tacacs-server host 172.16.1.1
```

**tacacs-server key**
The `tacacs-server key` Global Configuration mode command sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. To disable the key, use the `no` form of this command.

**Syntax**
```
tacacs-server key key-string
no tacacs-server key
```

- `key-string`—Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the encryption used on the TACACS daemon. (Range: 0 - 128 characters)

**Default Configuration**
Empty string

**Command Mode**
Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Examples**
The following example sets the authentication encryption key.

```
Console (config)# tacacs-server key dell-s
```

**tacacs-server timeout**
The `tacacs-server timeout` Global Configuration mode command sets the timeout value. To restore the default, use the `no` form of this command.

**Syntax**
```
tacacs-server timeout timeout
no tacacs-server timeout
```

- `timeout`—Specifies the timeout value. (Range: 0 - 3600 seconds)

---

328 | TACACS Commands
timeout—Specifies the timeout value in seconds. (Range: 1 - 30)

Default Configuration
5 seconds

Command Mode
Global Configuration mode

User Guidelines
• There are no user guidelines for this command.

Examples
The following example sets the timeout value as 30.

```
Console (config)# tacacs-server timeout 30
```

tacacs-server source-ip
The `tacacs-server source-ip` Global Configuration mode command specifies the source IP address that will be used for the communication with TACACS servers. To return to default, use the `no` form of this command.

**Syntax**
```
tacacs-server source-ip source
no tacacs-server source-ip source
```

• `source`—Specifies the source IP address. (Range: Valid IP Address)

Default Configuration
The IP address would be of the outgoing IP interface.

Command Mode
Global Configuration mode

User Guidelines
• There are no user guidelines for this command.

Examples
The following example specifies the source IP address.

```
Console (config)# tacacs-server source-ip 172.16.8.1
```
show tacacs
The show tacacs Privileged EXEC mode command displays configuration and statistics for a TACACS+ server.

Syntax
  show tacacs [ip-address]
  • ip-address—Name or IP address of the host.

Default Configuration
  This command has no default configuration.

Command Mode
  Privileged EXEC mode

User Guidelines
  • There are no user guidelines for this command.

Examples
The following example displays configuration and statistic for a TACACS+ server.

```
Console# show tacacs
IP address Status Port Single Connection TimeOut Source IP Priority
------------ ------- ----- -------------- ------- ------- ------- -------
172.16.1.1 Connected 49  No Global Global 1

Global values
-------------
TimeOut: 3
Source IP: 172.16.8.1
```
User Interface

enable
The enable User EXEC mode command enters the privileged EXEC mode.

Syntax
   enable [privilege-level]
   •  privilege-level—Privilege level to enter the system. (Range: 1 - 15)

Default Configuration
   The default privilege level is 15.

Command Mode
   User EXEC mode

User Guidelines
   •  There are no user guidelines for this command.

Example
The following example shows how to enter privileged mode:

  Console> enable
  enter password:
  Console#

disable
The disable Privileged EXEC mode command returns to User EXEC mode.

Syntax
   disable [privilege-level]
   •  privilege-level—Privilege level to enter the system. (Range: 1 - 15)

Default Configuration
   The default privilege level is 1.

Command Mode
   Privileged EXEC mode
User Guidelines

- There are no user guidelines for this command.

Example
The following example shows how to return to normal mode.

```
Console# disable
Console>
```

`login`

The `login` User EXEC mode command changes a login username.

Syntax

```
login
```

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- There are no user guidelines for this command.

Example

The following example shows how to enter privileged EXEC mode and login.

```
Console> login
User Name:admin
Password:*****
```

`configure`

The `configure` Privileged EXEC mode command enters the global configuration mode.

Syntax

```
configure
```

This command has no keywords or arguments.
**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
In the following example, because no keyword is entered, a prompt is displayed. After the keyword is selected, a message confirming the command entry method is displayed.

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

**exit(configuration)**
The `exit` command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

**Syntax**
- `exit`

**Default Configuration**
This command has no default configuration.

**Command Mode**
All command modes

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example changes the configuration mode from Interface Configuration mode to User EXEC mode.

```text
Console(config-if)# exit
Console(config)# exit
Console#
```
exit (EXEC)

The `exit` User EXEC mode command closes an active terminal session by logging off the device.

**Syntax**

```plaintext
exit
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example closes an active terminal session.

```plaintext
Console> exit
```

end

The `end` Global Configuration mode command ends the current configuration session and returns to the privileged command mode.

**Syntax**

```plaintext
end
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

All Command modes

**User Guidelines**

- There are no user guidelines for this command.
**Example**

The following example ends the current configuration session and returns to the previous command mode.

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

**help**

The `help` command displays a brief description of the help system.

**Syntax**

```
help
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

All Command modes

**User Guidelines**

- There are no user guidelines for this command.

**history**

The `history` Line Configuration mode command enables the command history function. To disable the command history feature, use the `no` form of this command.

**Syntax**

```
history
no history
```

**Default Configuration**

The history function is enabled.

**Command Mode**

Line Configuration mode

**User Guidelines**

- There are no user guidelines for this command.
**Example**
The following example enables the command history function for telnet.

```
Console (config)# line telnet
Console (config-line)# history
```

**history size**
The `history size` Line Configuration mode command changes the command history buffer size for a particular line. To reset the command history buffer size to the default, use the `no` form of this command.

**Syntax**

```
history size number-of-commands
no history size
```

- `number-of-commands`—Number of commands that the system records in its history buffer. (Range: 0 - 256)

**Default Configuration**
The default history buffer size is 10.

**Command Mode**
Line Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example changes the command history buffer size to 100 entries for a particular line.

```
Console (config-line)# history size 100
```

**debug-mode**
The `debug-mode` Privilege EXEC mode command switches the mode to debug.

**Syntax**

```
debug-mode
```

**Default Configuration**
This command has no default configuration.
**Command Mode**
Privilege EXEC command mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example enables the debug command interface.

```
console(config)#
console# debug
>debug
Enter DEBUG Password: ******
DEBUG>
```

**show history**
The `show history` User EXEC mode command lists the commands entered in the current session.

**Syntax**
```
show history
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
User EXEC command mode

**User Guidelines**
- The commands are listed from the first to the latest command.
- The buffer is unchanged when entering to configuration mode and returning back.
- The command in the buffer includes the commands that were not executed.
Example
The following example displays all the commands entered while in the current privileged EXEC mode.

```
Console# show history
show version
show clock
show history
```

show privilege
The `show privilege` User EXEC mode command displays the current privilege level.

Syntax
  `show privilege`

Default Configuration
  This command has no default configuration.

Command Mode
  User EXEC command mode

User Guidelines
  - There are no user guidelines for this command.

Example
The following example displays the current privilege level.

```
Console# show privilege
Current privilege level is 15
```
VLAN Commands

**vlan database**
The `vlan database` Global Configuration mode command enters the VLAN configuration mode.

**Syntax**
```
vlan database
```

**Default Configuration**
This command has no default configuration.

**Command Mode**
Global Configuration mode

**User Guidelines**
- There are no user guidelines for this command.

**Example**
The following example enters the VLAN database mode.

```console
Console (config)# vlan database
Console (config-vlan)#
```

**vlan**
Use the `vlan` VLAN Configuration mode command to create a VLAN. To delete a VLAN, use the `no` form of this command.

**Syntax**
```
vlan (vlan-range)
no vlan (vlan-range)
```

- `vlan-range`—A list of valid VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas (without spaces); use a hyphen to designate a range of IDs. (Range: 2 - 4094)

**Default Configuration**
This command has no default configuration.

**Command Mode**
VLAN Configuration mode
User Guidelines

- There are no user guidelines for this command.

Example

The following example VLAN number 1972 is created.

```
Console (config)# vlan database
Console (config-vlan)# vlan 1972
```

default-vlan disable

The default-vlan disable VLAN Configuration mode command disables the default VLAN functionality. Use the no form of this command to enable the default VLAN functionality.

Syntax

```
default-vlan disable

no default-vlan disable
```

This command has no keywords or arguments.

Default Configuration

Enabled

Command Modes

VLAN Configuration mode

User Guidelines

- There are no user guidelines for this command.

Examples

```
Console# vlan database
Console(config-vlan)# default-vlan disable
```

interface vlan

The interface vlan Global Configuration mode command enters the interface configuration (VLAN) mode.

Syntax

```
interface vlan vlan-id
```

- `vlan-id`—The ID of an existing VLAN (excluding GVRP dynamic VLANs).
Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
- There are no user guidelines for this command.

Example
The following example configures the VLAN 1 IP address of 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

interface range vlan
The `interface range vlan` Global Configuration mode command enters the interface configuration
mode to configure multiple VLANs.

Syntax
```
interface range vlan {vlan-range | all}
```
- `vlan-range`—A list of valid VLAN IDs to add. Separate non consecutive VLAN IDs with a
  comma and no spaces; a hyphen designates a range of IDs.
- `all`—All existing static VLANs.

Default Configuration
This command has no default configuration.

Command Mode
Global Configuration mode

User Guidelines
- Commands under the interface range context are executed independently on each interface
  in the range. If the command returns an error on one of the interfaces, an error message is
  displayed and execution continues on other interfaces.
Example
The following example groups VLAN 221 until 228 and VLAN 889 to receive the same command.

```
Console (config)# interface range vlan 221-228,889
Console (config-if)#
```

name
The `name` Interface Configuration mode command adds a name to a VLAN. To remove the VLAN name use the `no` form of this command.

**Syntax**

```
name string
no name
```

- `string`—Unique name, up to 32 characters in length, to be associated with this VLAN.

**Default Configuration**

No name is defined.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

- The VLAN name should be unique.

**Example**

The following example names VLAN number 19 with the name "Marketing".

```
Console (config)# interface vlan 19
Console (config-if)# name Marketing
```

switchport access vlan

The `switchport access vlan` Interface Configuration mode command configures the VLAN ID when the interface is in access mode. To reconfigure the default, use the `no` form of this command.

**Syntax**

```
switchport access vlan vlan-id
no switchport access vlan
```

- `vlan-id`—VID of the VLAN to which the port is configured.
Default Configuration

VID=1

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

• The command automatically removes the port from the previous VLAN, and adds it to the new VLAN.

Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN interface number g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport access vlan 23
```

switchport trunk allowed vlan

The `switchport trunk allowed vlan` Interface Configuration mode command adds or removes VLANs, to or from a trunk port.

Syntax

```
switchport trunk allowed vlan {add vlan-list | remove vlan-list}
```

• `add vlan-list`—List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

• `remove vlan-list`—List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

• There are no user guidelines for this command.
Example
The following example shows how to add VLANs 2 and 5 to 8 to the allowed list of g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport trunk allowed vlan add 2,5-8
```

**switchport trunk native vlan**
The `switchport trunk native vlan` Interface Configuration mode command defines the port as a member of the specified VLAN, and the VLAN ID as the "port default VLAN ID (PVID)". To configure the default VLAN ID, use the `no` form of this command.

**Syntax**
```
switchport trunk native vlan vlan-id
no switchport trunk native vlan
```

- `vlan-id`—Valid VLAN ID of the native VLAN.

**Default Configuration**
If default VLAN is enabled, then the VID=1, otherwise VID = 4095.

**Command Mode**
Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**
- This command has the following consequences: incoming untagged frames are assigned to this VLAN and outgoing traffic in this VLAN on this port is sent untagged (despite the normal situation where traffic sent from a trunk-mode port is all tagged).
- The command adds the port as a member in the VLAN. If the port is already a member in the VLAN (not as a native), it should be first removed from the VLAN.

**Example**
The following example g8, in trunk mode, is configured to use VLAN number 123 as the "native" VLAN.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport trunk native vlan 123
```

**switchport general allowed vlan**
The `switchport general allowed vlan` Interface Configuration mode command adds or removes VLANs from a general port.
Syntax

```
switchport general allowed vlan add vlan-list [tagged | untagged]
```

```
switchport general allowed vlan remove vlan-list
```

- `add vlan-list` — List of VLAN IDs to add. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- `remove vlan-list` — List of VLAN IDs to remove. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- `tagged` — Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged the default is tagged.
- `untagged` — Sets the port to transmit untagged packets for the VLANs.

Default Configuration
This command has no default configuration.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
- You can use this command to change the egress rule (e.g. from tagged to untagged), without first removing the VLAN from the list.

Example
The following example shows how to add VLANs 2, 5, and 6 to the allowed list.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general allowed vlan add 2,5,6 tagged
```

**switchport general pvid**

The `switchport general pvid` Interface Configuration mode command configures the PVID when the interface is in general mode. To configure the default value, use the `no` form of this command.

Syntax

```
switchport general pvid vlan-id
```

```
no switchport general pvid
```

- `vlan-id` — PVID (Port VLAN ID). The vlan-id may belong to a non-existent VLAN.

Default Configuration
VLAN ID = 1
**Command Mode**

Interface configuration (Ethernet, port-channel) mode

**User Guidelines**

- This command has the following consequences: incoming untagged frames are assigned to this VLAN and outgoing traffic in this VLAN on this port is sent untagged (despite the normal situation where traffic sent from a trunk-mode port is all tagged).

**Example**

The following example shows how to configure the PVID for g8, when the interface is in general mode.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general pvid 234
```

**switchport general ingress-filtering disable**

The `switchport general ingress-filtering disable` Interface Configuration mode command disables port ingress filtering. To enable ingress filtering on a port, use the `no` form of this command.

**Syntax**

```
switchport general ingress-filtering disable
no switchport general ingress-filtering disable
```

**Default Configuration**

Ingress filtering is enabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example shows how to enable port ingress filtering on g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general ingress-filtering disable
```
switchport general acceptable-frame-type tagged-only

The switchport general acceptable-frame-type tagged-only Interface Configuration mode command discards untagged frames at ingress. To enable untagged frames at ingress, use the no form of this command.

Syntax

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

• There are no user guidelines for this command.

Example

The following example configures g8 to discard untagged frames at ingress.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general acceptable-frame-type tagged-only
```

switchport forbidden vlan

The switchport forbidden vlan Interface Configuration mode command forbids adding specific VLANs to a port. This may be used to prevent GVRP from automatically making these VLANs active on the selected ports. To revert to allowing the addition of specific VLANs to the port, use the remove parameter for this command.

Syntax

switchport forbidden vlan {add vlan-list | remove vlan-list}

• add vlan-list—List of VLAN IDs to add to the "forbidden" list. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

• remove vlan-list—List of VLAN IDs to remove from the "forbidden" list. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

All VLANs allowed.
map protocol protocols-group

The `map protocol protocols-group` VLAN Configuration mode command maps a protocol to a protocol group. Protocol groups are used for protocol-based VLAN assignment. To delete a protocol from a group, use the no form of this command.

**Syntax**

```
map protocol protocol [encapsulation] protocols-group group
no map protocol protocol encapsulation
```

- `protocol`—The protocol is a 16 or 40 bits protocol number or one of the following names, `ip-arp` or `ipx`. The protocol number is in Hex format (Range: 0600 - FFFF).
- `encapsulation`—One of the following values: `ethernet`, `rfc1042` or `llcOther`. If no option is indicated the default is `ethernet`.
- `group`—Protocol group number (Range: 1 - 2147483647).

**Default Configuration**

This command has no default configuration.

---

### VLAN Commands

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example forbids adding VLANs number 234 till 256, to g8.

```plaintext
Console (config)# interface ethernet g8
Console (config-if)# switchport forbidden vlan add 234-256
```

**map protocol protocols-group**

The `map protocol protocols-group` VLAN Configuration mode command maps a protocol to a protocol group. Protocol groups are used for protocol-based VLAN assignment. To delete a protocol from a group, use the no form of this command.

**Syntax**

```
map protocol protocol [encapsulation] protocols-group group
no map protocol protocol encapsulation
```

- `protocol`—The protocol is a 16 or 40 bits protocol number or one of the following names, `ip-arp` or `ipx`. The protocol number is in Hex format (Range: 0600 - FFFF).
- `encapsulation`—One of the following values: `ethernet`, `rfc1042` or `llcOther`. If no option is indicated the default is `ethernet`.
- `group`—Protocol group number (Range: 1 - 2147483647).

**Default Configuration**

This command has no default configuration.

**Command Mode**

VLAN Configuration mode

**User Guidelines**

- There are no user guidelines for this command

**Example**

The following example maps protocol ip-arp to the group named "213".

```plaintext
Console (config)# vlan database
Console (config-vlan)# map protocol ip-arp protocols-group 213
```
**switchport general map protocols-group vlan**

The `switchport general map protocols-group vlan` Interface Configuration mode command sets a protocol-based classification rule. To delete a classification, use the `no` form of this command.

**Syntax**

```
switchport general map protocols-group group vlan vlan-id
no switchport general map protocols-group group
```

- `group`—Group number as defined in the `map protocol protocols-group` command. (Range: 1 - 2147483647)
- `vlan-id`—Define the VLAN ID in the classifying rule.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example sets a protocol-based classification rule of protocol group 1 to VLAN 8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

**ip internal-usage-vlan**

The `ip internal-usage-vlan` Interface Configuration mode command reserves a VLAN as the internal usage VLAN of an interface. Use the `no` form of this command to reset to default.

**Syntax**

```
ip internal-usage-vlan vlan-id
no ip internal-usage-vlan
```

- `vlan-id`—VLAN ID of the internal usage VLAN. (Range: Valid VLAN)

**Default Configuration**

This command has no default configuration.
**Command Mode**

Interface configuration (Ethernet, port-channel)

**User Guidelines**

- An internal usage VLAN is required when an IP interface is defined on Ethernet port or Port-channel.
- Using this command the user can define the internal usage VLAN of a port.
- If an internal-usage is not defined for a Port, and the user wants to define an IP interface, the software chooses one of the unused VLANs.
- If a VLAN ID was chosen by the software for internal usage, and the user wants to use that VLAN ID for static or dynamic VLAN, he should either remove the IP interface, creates the VLAN, and recreate the IP interface, or use this command to define explicit internal usage VLAN.

**Examples**

The following example reserves a VLAN as the internal usage VLAN of an interface.

```
Console (config)# ip internal-usage-vlan 10
```

**show vlan**

The `show vlan` Privileged EXEC mode command displays VLAN information.

**Syntax**

```
show vlan [tag vlan-id | name vlan-name]
```

- `vlan-id`—A valid VLAN ID
- `vlan-name`—A valid VLAN name string. (Range: 1 - 32 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays all VLAN information.
show vlan internal usage

The `show vlan internal usage` Privileged EXEC mode command displays a list of VLANs being used internally by the switch.

**Syntax**

```
show vlan internal usage
```  

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.
**Example**

The following example displays all VLAN information.

```
Console# show vlan internal usage
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Usage</th>
<th>Reserved</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1007</td>
<td>g21</td>
<td>No</td>
<td>Active</td>
</tr>
<tr>
<td>1008</td>
<td>g22</td>
<td>Yes</td>
<td>Inactive</td>
</tr>
<tr>
<td>1009</td>
<td>g23</td>
<td>Yes</td>
<td>Active</td>
</tr>
</tbody>
</table>
```

**show vlan protocols-groups**

The `show vlan protocols-groups` Privileged EXEC mode command displays protocols-groups information.

**Syntax**

```
show vlan protocols-groups
```

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays protocols-groups information.
show interfaces switchport

The show interfaces switchport Privileged EXEC mode command displays switchport configuration.

**Syntax**

```
show interfaces switchport {ethernet interface | port-channel port-channel-number}
```

- **Interface**—Specific interface, such as ethernet g8.
- **port-channel-number**—Valid port-channel trunk index.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays switchport configuration individually for g1.
VLAN Commands

switchport mode

Use the `switchport mode` interface configuration command to configure the VLAN membership mode of a port. Use the no form of this command to reset the mode to the appropriate default for the device.

**Syntax**

```
switchport mode {customer | access | trunk | general}
```
no switchport mode

- **customer** — The port is connected to customer equipment. Used when the switch is in a provider network.
- **access** — Untagged layer 2 VLAN interface
- **trunk** — Trunking layer 2 VLAN interface
- **general** — Full 802.1q support VLAN interface

**Default Configuration**

All ports are in access mode, and belong to the default VLAN (whose VID=1).

**Command Modes**

Interface configuration (Ethernet, port-channel)

**User Guidelines**

- There are no user guidelines for this command

**Example**

The following example configures the VLAN membership mode of a port. Use the no form of this command to reset the mode to the appropriate default for the device.

```
console# config
console(config)# interface ethernet g1
console(config-if)# switchport mode customer
```

**switchport customer vlan**

Use the `switchport customer vlan` interface configuration command to set the port's VLAN when the interface is in customer mode. Use the `no` form of this command to revert to default.

**Syntax**

```
switchport customer vlan vlan-id
no switchport customer vlan
```

- **vlan-id** — VLAN ID of the customer

**Default Configuration**

No VLAN is configured.

**Command Modes**

Interface configuration (Ethernet, port-channel)
**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example sets the port’s VLAN when the interface is in customer mode.

```console
Console(config)# interface ethernet g5
Console(config-if)# switchport customer vlan vlan-id
```
Web Server

ip http server
The `iphttp server` Global Configuration mode command enables the device to be configured from a browser. To disable this function use the `no` form of this command.

Syntax
- `ip http server`
- `no ip http server`

Default Configuration
HTTP server is disabled by default.

Command Mode
Global Configuration mode

User Guidelines
- Only a user with access level 15 can use the web server.

Example
The following example enables the device to be configured from a browser.

```
Console (enable)# ip http server
```

ip http port
The `ip http port` Global Configuration mode command specifies the TCP port for use by a web browser to configure the device. To use the default TCP port, use the `no` form of this command.

Syntax
- `ip http port port-number`
- `no ip http port`
  - `port-number`—Port number for use by the HTTP server. (Range: 0 - 65535)

Default Configuration
This default port number is 80.

Command Mode
Global Configuration mode
User Guidelines

- There are no user guidelines for this command. However, specifying 0 as the port number will effectively disable HTTP access to the device.

Example

The following example shows how the http port number is configured to 100.

```
Console (config)# ip http port 100
```

ip https server

The `ip https server` Global Configuration mode command enables the device to be configured from a secured browser. To disable this function, use the `no` form of this command.

Syntax

```
ip https server
no ip https server
```

Default Configuration

The default for the device is disabled.

Command Mode

Global Configuration mode

User Guidelines

- You must use the `crypto certificate generate` command to generate the HTTPS certificate.

Example

The following example enables the device to be configured from a browser.

```
Console (enable)# ip https server
```

ip https port

The `ip https port` Global Configuration mode command configures a TCP port for use by a secure web browser to configure the device. To use the default port, use the `no` form of this command.

Syntax

```
ip https port port-number
no ip https port
```

- `port-number`—Port number for use by the HTTP server. (Range: 0 - 65535)
Default Configuration
This default port number is 443.

Command Mode
Global Configuration mode

User Guidelines
• There are no user guidelines for this command.

Example
The following example configures the https port number to 100.

```
Console (enable)# ip https port 100
```

crypto certificate generate
The crypto certificate generate Global Configuration mode command generates a HTTPS certificate.

Syntax
```
crypto certificate [number] generate [key-generate [length]] [passphrase string] [en common-name] [ou organization-unit] [o organization] [l location] [st state] [c country] [duration days]
```

• `number` — Specifies the certificate number. If unspecified, defaults to 1. (Range: 1 - 2)
• `key-generate` — Regenerate SSL RSA key.
• `length` — Specifies the SSL RSA key length. If unspecified, length defaults to 1024. (Range: 512 - 2048)
• `passphrase string` — Passphrase that is used for exporting the certificate in PKCS12 file format. If unspecified the certificate is not exportable. (Range: 8 - 96)
• `en common-name` — Specifies the fully qualified URL or IP address of the device. If unspecified, defaults to the lowest IP address of the device (where the certificate is generated). (Range: 1 - 64)
• `ou organization-unit` — Specifies the organization-unit or department name. (Range: 1 - 64)
• `o organization` — Specifies the organization name. (Range: 1 - 64)
• `l location` — Specifies the location or city name. (Range: 1 - 64)
• `st state` — Specifies the state or province name. (Range: 1 - 64)
• `c country` — Specifies the country name. (Range: 1 - 2)
• `duration days` — Specifies number of days a certification would be valid. If unspecified defaults to 365 days. (Range: 30 - 3650)
**Default Configuration**
The Certificate and the SSL RSA key pairs do not exist.

**Command Mode**
Global Configuration mode

**User Guidelines**
- The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up to another device.
- Use this command to generate self-signed certificate for your device.
- When you export an RSA key pair to a PKCS#12 file, the RSA key pair is as secure as the passphrase. Therefore, keep the passphrase secure.

**Example**
The following example regenerates a HTTPS certificate.
```
Console (enable)# crypto certificate generate key-generate
```

**crypto certificate request**
The `crypto certificate request` Privileged EXEC mode command generates and displays certificate requests for HTTPS.

**Syntax**
```
crypto certificate number request common-name [ou organization-unit] [o organization] [l location] [st state] [c country]
```
- `number`—Specifies the certificate number. (Range: 1 - 2)
- `common-name`—Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- `ou organization-unit`—Specifies the organization-unit or department name. (Range: 1-64)
- `o organization`—Specifies the organization name. (Range: 1-64)
- `l location`—Specifies the location or city name. (Range: 1-64)
- `st state`—Specifies the state or province name. (Range: 1-64)
- `c country`—Specifies the country name. (Range: 1-2)

**Default Configuration**
There is no default configuration for this command.
Command Mode
Privileged EXEC mode

User Guidelines

- Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.
- Before generating a certificate request you must first generate a self-signed certificate using the `crypto certificate generate` Global Configuration mode command.
- After receiving the certificate from the Certification Authority, use the `crypto certificate import` Global Configuration mode command to import the certificate into the device. This certificate would replace the self-signed certificate.

Examples
The following example generates and displays a certificate request for HTTPS.

```
Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAXCzA JBgNVBAoTAmNQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzA JBgNVBAMTAmNQ
DgKoZIhvcNAQkJBPgFsMIGfMA0GCSqGSIb3DQEBAQUA4GNADCBiQKBgQ
Hp/igVPmFM+1nbqTDekb2ymCu6K
-----END CERTIFICATE REQUEST-----
```

CN= router.gm.com
O= General Motors
C= US
**crypto certificate import**

The `crypto certificate import` Global Configuration mode command imports a certificate signed by Certification Authority for HTTPS.

**Syntax**

```
crypto certificate number import
```

- `number`—Specifies the certificate number. (Range: 1 - 2)

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Global configuration mode

**User Guidelines**

- Use this command to enter an external certificate (signed by Certification Authority) to the device. To end the session, enter a new line, enter "." (period) and add another new line.
- The imported certificate must be based on a certificate request created by the `crypto certificate request` Privileged EXEC mode command.
- If the public key found in the certificate does not match the device’s SSL RSA key, the command will fail.
- This command is not saved in the device configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).
Examples
The following example imports a certificate signed by Certification Authority for HTTPS.

Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
DHmUgUm9vdCBDZXJ0aWZpZXIxNDANBgkqhkiG9w0BAQEFAANLADBI AskEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTmlxyJ1t11a1GaqchfMqge0kmfhcoHSWr
yflFpD0MWOTgDAwIDAQABo4IBojCCA43wEwYJKwYBBAGCNxQCBAYeBABAEEw
Cw0PBAQDAAgFGMA8GA1UdEwEB/wQFMAMBAf5wHQYDVR0BAIIBEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIBLTCCASkwdKgc+ggcyGgc1sZGFwOi8v
L0VByb3h5JTIwU29mdHdcmUlMjBsb290JTIwQ2VydGlmaWVyLENOPXN1cnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788

ip https certificate

The **ip https certificate** Global Configuration mode command configures the active certificate for HTTPS. Use the **no** form of this command to return to default.

**Syntax**
```
ip https certificate number
no ip https certificate
```

- **number**—Specifies the certificate number. (Range: 1 - 2)

**Default Configuration**
Certificate number 1.
**Command Mode**

Global configuration mode

**User Guidelines**

- The `crypto certificate generate` command should be used in order to generate HTTPS certificates.

**Example**

The following example configures the active certificate for HTTPS.

```
Console (config)# ip https certificate 1
```

**crypto certificate export pkcs12**

The `crypto certificate export pkcs12` Privileged EXEC mode command, exports the certificate and the RSA keys within a PKCS12 file.

**Syntax**

```
crypto certificate number export pkcs12
```

- `number`—Specifies the certificate number. (Range: 1 - 2)

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- The `crypto certificate export pkcs12` command creates a PKCS 12 file that contains the certificate and an RSA key pair.
- The passphrase for the exporting is determined when the key is generated.
- The certificate and key pair is exported in standard PEM-format PKCS12 file. This format can be converted to and from the binary PFX file used by Windows and Linux by using the openssl command-line tool. See the OpenSSL user manual (man pkcs12) for more information.
Example
The following example exports the certificate and RSA keys.

```
Console# crypto certificate 1 export pkcs12
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject= /C=us/ST= /L= /CN= /O= /OU=
 issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAgTASAxCjAIgNVBAcTAkSAXCjAIGNVBAoTASAxCjAIgNVBAIhCnMDAwMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBQMQswCQYDVQQG
BwJ1czEKMgQGA1UEBhMCc3Nwb3N0MQswCQYDVQQH
-----END CERTIFICATE-----

-----END RSA PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAgTASAxCjAIgNVBAcTAkSAXCjAIGNVBAoTASAxCjAIgNVBAIhCnMDAwMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBQMQswCQYDVQQG
BwJ1czEKMgQGA1UEBhMCc3Nwb3N0MQswCQYDVQQH
-----END CERTIFICATE-----
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-ED3-CBC, 085DCBF3A41D2669
dac0m9jqEp1DM50aD8Bj1jxw/1PkgSxuMhc25odBE/1fPBg9V$V1ARaYt16W
bX67UyJ8t7HHFJAcwjcWzElQg5QjgSQ1VemsqaR0qThisCTb090rx+cNwWfIVjoedQ
Mt15+fKIAcsfEgEGfUXQ4jEdsXakw3QLFggt47031pUn0A$x2QzutJDoC28Ux
raMVTV1SjIvaPuAXjxd27ZtDMvZffILb1KjGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXb/3h4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYR7+7JXLKhp
dueu3znfIX4dDeti8832x$yv8kGZjxFN1cC3zc3JsD0IVlLkyiAa93P4LEvAwG
Fw1LqmGiiqw9JM/zzc6kYkZXY1FczSvF2xp+/tEvM=
-----END RSA PRIVATE KEY-----
```
**crypto certificate import pkcs12**

The crypto certificate import pkcs12 Privileged EXEC mode command, imports the certificate and the RSA keys within a PKCS12 file.

**Syntax**

```
crypto certificate number import pkcs12 passphrase
```

- `number`—Specifies the certificate number. (Range: 1 - 2)
- `passphrase`—Passphrase that is used to encrypt the PKCS12 file for export. (Range: 8 - 96)

**Default Configuration**

There is no default configuration for this command.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- The passphrase that was exported by the crypto certificate export pkcs12 command should be used. Please note that this passphrase would be saved for later exports.

**Example**

The following example imports the certificate and RSA keys.
console# crypto certificate 1 import pkcs12 passphrase

Bag Attributes

localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4

-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAgTASAxCjAIBgNVBAcTASAxCjAIBgNVBAoTASAxCjAIBgNV
BAstTASAwHhcNMDQwMja3MTU1NDQ4WhcNMDUwMja2MTU1NDQ4WjBJMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMBbDEFKMAgGA1UECBMBbDEFKMAgGA1UECBMBbDEFKMAgGA1UE
ChMBDEFKMAgGA1UECnxMBfDEFKMAgGA1UECnxMBfDEFKMAgGA1UECnxMBfDEFKMAgGA1UE
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxW/1P0kgSxuMhc250dBE/1fPBg9VSvV1ARaYt16W
bx67UyJ8t7H5F3AowjcwZlQ5OjgQ0VemsqsRQzjpCTb090rx+cNwVfVjonedqQ
Mt15+fKIAcqsfeG6JNXQ4jEzaXAkwqQLFfgt47O3IpUn0AxxQzutJD0cCz8Uxp
raMVTVS1skJivaPuXzd2Z79tDMw2zfILbFKCGJCACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyy2Spw9BPPR/8bc/wUYERh7t+7JXLKhp
ueeu3znfIX4dDet1833xYyvve8KZjxjFn1cCzcz3JsD0IVu1LkyiAa93P4LPevAwG
Fw1LgmiGiiqw9JM/tz6cYkZXy1FzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----
show crypto certificate mycertificate

The `show crypto certificate mycertificate` Privileged EXEC mode command allows you to view the SSL certificates of your device.

**Syntax**

```
show crypto certificate mycertificate [number]
```

- `number`—Specifies the certificate number. (Range: 1-2)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the certificate.

```
Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
... 
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
-----END CERTIFICATE-----
```
show ip http
The show ip http Privileged EXEC mode command displays the HTTP server configuration.

Syntax
   show ip http

Default Configuration
   This command has no default configuration.

Command Mode
   Privileged EXEC mode

User Guidelines
   • There are no user guidelines for this command.

Example
The following example displays the HTTP server configuration.

Console# show ip http
HTTP server enabled. Port: 80

show ip https
The show ip https Privileged EXEC mode command displays the HTTPS server configuration.

Syntax
   show ip https

Default Configuration
   This command has no default configuration.

Command Mode
   Privileged EXEC mode

User Guidelines
   • There are no user guidelines for this command.
**Example**
The following example displays the HTTP server configuration.

```plaintext
Console# `show ip https`
HTTPS server enabled. Port: 443

Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```
aaa authentication dot1x

The aaa authentication dot1x Global Configuration mode command specifies one or more authentication, authorization, and accounting (AAA) methods for use to authenticate interfaces running IEEE 802.1X. Use the no form of this command to return to default.

**Syntax**

```
aaa authentication dot1x default method1 [method2...]
```

```
no aaa authentication dot1x default
```

- `method1 [method2...]`—At least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius</td>
<td>Uses the list of all RADIUS servers for authentication</td>
</tr>
<tr>
<td>None</td>
<td>Uses no authentication</td>
</tr>
</tbody>
</table>

**Default Configuration**

The default behavior of the "aaa authentication" for dot1.x is "failed to authenticate". If the 8021.x calls the AAA for authentication services it will receive a fail status.

**Command Mode**

Global configuration mode

**User Guidelines**

- The additional methods of authentication are used only if the previous method returns an error, for example the authentication server is down, and not if the request for authenticate is denied access. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

- The radius server must support MD-5 challenge and EAP type frames.

**Examples**

The following example uses the aaa authentication dot1x default command with no authentication.

```
Console (config)# aaa authentication dot1x default none
```
**dot1x system-auto-control**

The `dot1x system-auto-control` Global Configuration mode command enables 802.1x globally. Use the `no` form of this command to disable 802.1x globally.

**Syntax**

```
dot1x system-auto-control
no dot1x system-auto-control
```

- This command has no arguments or keywords.

**Default Configuration**

Disabled

**Command Modes**

Global configuration mode

**User Guidelines**

- There are no user guidelines for this command.

**Examples**

The following example enables 802.1x globally.

```
Console (config)# dot1x system-auto-control
```

**dot1x port-control**

The `dot1x port-control` Interface Configuration mode command enables manual control of the authorization state of the port. Use the `no` form of this command to return to the default setting.

**Syntax**

```
dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control
```

- `auto`—Enable 802.1X authentication on the interface and cause the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.
- `force-authorized`—Disable 802.1X authentication on the interface and cause the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1X-based authentication of the client.
- `force-unauthorized`—Deny all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
Default Configuration
force-authorized

Command Mode
Interface configuration (Ethernet)

User Guidelines
- It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1X edge ports (ports in auto state that are connected to end stations), in order to get immediately to the forwarding state after successful authentication.

Examples
The following example enables 802.1X authentication on the interface.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x port-control auto
```

dot1x re-authentication
The `dot1x re-authentication` Interface Configuration mode command enables periodic re-authentication of the client. Use the `no` form of this command to return to the default setting.

Syntax
```
dot1x re-authentication
no dot1x re-authentication
```

This command has no arguments or keywords.

Default Configuration
Periodic re-authentication is disabled.

Command Mode
Interface configuration (Ethernet)

User Guidelines
- It is recommended to use re-authentication because if re-authentication is not defined, once a port is authenticated, it will remain in this state until the port is down or a log-off message is sent by client.
Examples
The following example enables periodic re-authentication of the client.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x re-authentication
```

dot1x timeout re-authperiod
The `dot1x timeout re-authperiod` Interface Configuration mode command sets the number of seconds between re-authentication attempts. Use the `no` form of this command to return to the default setting.

Syntax
```
dot1x timeout re-authperiod seconds
no dot1x timeout re-authperiod
```

- `seconds`— Number of seconds between re-authentication attempts. (Range: 300 - 4294967295)

Default Configuration
3600

Command Mode
Interface configuration (Ethernet) mode

User Guidelines
- There are no user guidelines for this command.

Examples
The following example sets the number of seconds between re-authentication attempts, to 3600.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x timeout re-authperiod 3600
```

dot1x re-authenticate
The `dot1x re-authenticate` Privileged EXEC mode command manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

```
dot1x re-authenticate [ethernet interface]
```

Default Configuration
This command has no default configuration.
802.1x Commands

Command Mode
Privileged EXEC mode

User Guidelines
There are no user guidelines for this command.

Examples
• The following command manually initiates a re-authentication of the 802.1X-enabled port.

  Console# dot1x re-authenticate ethernet g8

dot1x timeout quiet-period

The dot1x timeout quiet-period Interface Configuration mode command sets the number of
seconds that the switch remains in the quiet state following a failed authentication exchange (for
example, the client provided an invalid password). Use the no form of this command to return to
the default setting.

Syntax
  dot1x timeout quiet-period seconds
  no dot1x timeout quiet-period

  • seconds—Time in seconds that the switch remains in the quiet state following a failed
    authentication exchange with the client. (Range: 0 - 65535 seconds)

Default Configuration
60

Command Mode
Interface configuration (Ethernet)

User Guidelines
• During the quiet period, the switch does not accept or initiate any authentication requests.
• The default value of this command should only be changed to adjust for unusual
  circumstances, such as unreliable links or specific behavioral problems with certain clients
  and authentication servers.
• If it is necessary to provide a faster response time to the user, a smaller number than the
  default should be entered.
**Examples**
The following example sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange, to 3600.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x timeout quiet-period 3600
```

**dot1x timeout tx-period**
The `dot1x timeout tx-period` Interface Configuration mode command sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame, from the client, before resending the request. Use the `no` form of this command to return to the default setting.

**Syntax**
```
dot1x timeout tx-period seconds
```
```
no dot1x timeout tx-period
```

- `seconds`— Time in seconds that the switch should wait for a response to an EAP - request/identity frame from the client before resending the request. (Range: 1 - 65535 seconds)

**Default Configuration**
```
30
```

**Command Mode**
Interface configuration (Ethernet) mode

**User Guidelines**
- You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Examples**
The following command sets the number of seconds that the switch waits for a response to an EAP - request/identity frame, to 3600 seconds.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x timeout tx-period 3600
```
dot1x max-req

The **dot1x max-req** Interface Configuration mode command sets the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) - request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. Use the **no** form of this command to return to the default setting.

**Syntax**

```
dot1x max-req count

no dot1x max-req
```

- `count`—Number of times that the switch sends an EAP - request/identity frame before restarting the authentication process. (Range: 1 - 10)

**Default Configuration**

2

**Command Mode**

Interface configuration (Ethernet) mode

**User Guidelines**

- You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Examples**

The following example sets the number of times that the switch sends an EAP - request/identity frame, to 6.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x max-req 6
```

dot1x timeout supp-timeout

The **dot1x timeout supp-timeout** Interface Configuration mode command sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. Use the **no** form of this command to return to the default setting.

**Syntax**

```
dot1x timeout supp-timeout seconds

no dot1x timeout supp-timeout
```

- `seconds`—Time in seconds that the switch should wait for a response to an EAP-request frame from the client before resending the request. (Range: 1 - 65535 seconds)
Default Configuration

30

Command Mode
Interface configuration (Ethernet) mode

User Guidelines
- The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples
The following example sets the time for the retransmission of an EAP-request frame to the client, to 3600 seconds.

```
console config-if(Conf-VLAN)# dot1x timeout supp-timeout 3600
```

dot1x timeout server-timeout

The `dot1x timeout server-timeout` Interface Configuration mode command sets the time for the retransmission of packets to the authentication server. Use the `no` form of this command to return to the default setting.

Syntax
```
dot1x timeout server-timeout seconds
no dot1x timeout server-timeout
```

- `seconds`—Time in seconds that the switch should wait for a response from the authentication server before resending the request. (Range: 1 - 65535 seconds)

Default Configuration

30

Command Mode
Interface configuration (Ethernet) mode

User Guidelines
- There are no user guidelines for this command.
Examples
The following example sets the time for the retransmission of packets to the authentication server, to 3600 seconds.

```
Console (config)# dot1x timeout server-timeout 3600
```

show dot1x
The `show dot1x` Privileged EXEC mode command displays 802.1X status for the switch or for the specified interface.

Syntax
```
show dot1x [ethernet interface]
```
- `interface`—The full syntax is: port.

Default Configuration
This command has no default configuration.

Command Mode
Privileged EXEC mode

User Guidelines
- There are no user guidelines for this command.

Examples
The following example displays 802.1X status for the switch.

```
Console# show dot1x

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
<th>Reauth Control</th>
<th>Reauth Period</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>Auto</td>
<td>Authorized</td>
<td>Ena</td>
<td>3600</td>
<td>Bob</td>
</tr>
<tr>
<td>g2</td>
<td>Auto</td>
<td>Authorized</td>
<td>Ena</td>
<td>3600</td>
<td>John</td>
</tr>
<tr>
<td>g3</td>
<td>Auto</td>
<td>Unauthorized</td>
<td>Ena</td>
<td>3600</td>
<td>Clark</td>
</tr>
<tr>
<td>g4</td>
<td>Force-auth</td>
<td>Authorized</td>
<td>Dis</td>
<td>3600</td>
<td>n/a</td>
</tr>
</tbody>
</table>
```
Console# `show dot1x ethernet g3`

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
<th>Reauth Control</th>
<th>Reauth Period</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>g3</td>
<td>Auto</td>
<td>Unauthorized</td>
<td>Ena</td>
<td>3600</td>
<td>Clark</td>
</tr>
</tbody>
</table>

State: held
Quiet period: 60
Tx period: 30
Max req: 2
Login Time: n/a
Last Authentication: n/a
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Termination Cause: Supplicant logoff

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number.</td>
</tr>
<tr>
<td>Admin mode</td>
<td>The admin mode of the port. Possible values are: Force-auth, Force-unauth, Auto.</td>
</tr>
<tr>
<td>Oper mode</td>
<td>The oper mode of the port. Possible values are: Authorized, Unauthorized.</td>
</tr>
<tr>
<td>Reauth Control</td>
<td>Reauthentication control.</td>
</tr>
<tr>
<td>Reauth Period</td>
<td>Reauthentication period.</td>
</tr>
<tr>
<td>Username</td>
<td>The User-Name representing the identity of the Supplicant.</td>
</tr>
<tr>
<td>State</td>
<td>The current value of the Authenticator PAE state machine.</td>
</tr>
<tr>
<td>Quiet period</td>
<td>The number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).</td>
</tr>
<tr>
<td>Tx period</td>
<td>The number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.</td>
</tr>
</tbody>
</table>
show dot1x users

The **show dot1x users** Privileged EXEC mode command displays 802.1X users for the switch.

**Syntax**

```
show dot1x users [username username]
```

- `username`—Supplicant username (Range: 1-160 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays 802.1X users.

```
console# show dot1x users

<table>
<thead>
<tr>
<th>Username</th>
<th>Session Time</th>
<th>Last Auth</th>
<th>Auth Method</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>1d3h</td>
<td>58m</td>
<td>Remote</td>
<td>00:08:3b:79:87:87</td>
<td>g1</td>
</tr>
<tr>
<td>John</td>
<td>8h19m</td>
<td>2m</td>
<td>None</td>
<td>00:08:3b:89:31:27</td>
<td>g2</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max req</td>
<td>The maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client before restarting the authentication process.</td>
</tr>
<tr>
<td>Login Time</td>
<td>How long the user is logged in.</td>
</tr>
<tr>
<td>Last Authentication</td>
<td>Time since last authentication.</td>
</tr>
<tr>
<td>Mac address</td>
<td>The supplicant MAC address.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>The authentication method used to establish the session.</td>
</tr>
<tr>
<td>Termination Cause</td>
<td>The reason for the session termination.</td>
</tr>
</tbody>
</table>
The `show dot1x statistics` Privileged EXEC mode command displays 802.1X statistics for the specified interface.

**Syntax**
```
show dot1x statistics ethernet interface
```
- `interface`—The full syntax is: `port`.

**Default Configuration**
This command has no default configuration.

**Command Mode**
Privileged EXEC mode

**User Guidelines**
- There are no user guidelines for this command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The User-Name representing the identity of the Supplicant.</td>
</tr>
<tr>
<td>Login Time</td>
<td>How long the user is logged in.</td>
</tr>
<tr>
<td>Last Authentication</td>
<td>Time since last authentication.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>The authentication method used to establish the session.</td>
</tr>
<tr>
<td>Mac address</td>
<td>The supplicant MAC address.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface that the user is using.</td>
</tr>
</tbody>
</table>
Examples
The following example displays 802.1X statistics for the specified interface.

```
Switch# show dot1x statistics ethernet g1

EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 0008.3b79.8787
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EapolFramesRx</td>
<td>The number of valid EAPOL frames of any type that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolFramesTx</td>
<td>The number of EAPOL frames of any type that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EapolStartFramesRx</td>
<td>The number of EAPOL Start frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolLogoffFramesRx</td>
<td>The number of EAPOL Logoff frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespIdFramesRx</td>
<td>The number of EAP Resp/Id frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespFramesRx</td>
<td>The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqIdFramesTx</td>
<td>The number of EAP Req/Id frames that have been transmitted by this Authenticator.</td>
</tr>
</tbody>
</table>
ADVANCED FEATURES

dot1x auth-not-req

The `dot1x auth-not-req` VLAN Configuration mode command enables unauthorized users access to that VLAN. Use the `no` form of this command to disable the access.

**Syntax**

dot1x auth-not-req

`no dot1x auth-not-req`

This command has no arguments or keywords.

**Default Configuration**

User should be authorized to access the VLAN.

**Command Mode**

VLAN Configuration mode

**User Guidelines**

- An access port cannot be a member in an unauthenticated VLAN. The native VLAN of a trunk port cannot be an unauthenticated VLAN. For a general port, the PVID can be the Unauthenticated VLAN (although only tagged packets would be accepted in Unauthorized state.)

**Examples**

The following example enables unauthorized users access to the VLAN.

```
console config-if(Config-VLAN)# dot1x auth-not-req
```
**dot1x multiple-hosts**

The **dot1x multiple-hosts** Interface Configuration mode command allows multiple hosts (clients) on an 802.1X-authorized port, that has the **dot1x port-control** Interface Configuration mode command set to **auto**. Use the **no** form of this command to return to the default setting.

**Syntax**

```
dot1x multiple-hosts
no dot1x multiple-hosts
```

This command has no arguments or keywords.

**Default Configuration**

Multiple hosts are disabled. If a port would join a port-channel, the state would be multiple hosts as long as the port is member in the port-channel.

Multiple-hosts must be enabled if the user wants to disable ingress-filtering on this port.

**Command Mode**

Interface configuration (Ethernet) mode

**User Guidelines**

- This command enables the attachment of multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.
- For unauthenticated VLANs multiple hosts are always enabled.

**Examples**

The following command allows multiple hosts (clients) on an 802.1X-authorized port.

```
console config-if(Config-VLAN)#dot1x multiple-hosts
```

**dot1x single-host-violation**

The **dot1x single-host-violation** Interface Configuration mode command configures the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the **no** form of this command to return to default.

**Syntax**

```
dot1x single-host-violation {forward | discard | discard-shutdown} [trap seconds]
no port dot1x single-host-violation
```

```
console config-if(Config-VLAN)#dot1x single-host-violation discard
```
• **forward**—Forward frames with source addresses not the supplicant address, but do not
  learn the address.
• **discard**—Discard frames with source addresses not the supplicant address.
• **discard-shutdown**—Discard frames with source addresses not the supplicant address.
  The port is also shutdown.
• **trap seconds**—Send SNMP traps, and specifies the minimum time between consecutive
  traps. (Range: 1-1000000)

**Default Configuration**

Discard frames with source addresses not the supplicant address. No traps.

**Command Mode**

Interface configuration (Ethernet) mode

**User Guidelines**

• The command is relevant when Multiple hosts is disabled and the user has been successfully
  authenticated

**Examples**

The following example uses the forward action to forward frames with source addresses.

```console
console(config-if)# dot1x single-host-violation
forward trap 100
```

**show dot1x advanced**

The *show dot1x advanced* Privileged EXEC mode command displays 802.1X advanced features for
the switch or for the specified interface.

**Syntax**

```
show dot1x advanced [ethernet interface]
```

• **interface**—Ethernet interface

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**User Guidelines**

• There are no user guidelines for this command.
Examples
The following example displays 802.1X advanced features for the switch.

```
Switch# show dot1x advanced

Unauthenticated VLANs: 91, 92

Port       Multiple  Hosts
          -------    -------
g1         Disabled
          -------    -------
g2         Enabled

Switch# show dot1x advanced ethernet g1

Port       Multiple  Hosts
          -------    -------
g1         Disabled
          -------    -------
Single host parameters
Violation action: Discard
Trap: Enabled
Trap frequency: 100
Status: Single-host locked
Violations since last trap: 9
```
console# show dot1x advanced ethernet g1

Guest VLAN: 3978
Unauthenticated VLANs: 91, 92
Use user attributes from Authentication Server: Enabled
User VLAN not created: Create
Interface       Multiple
                Hosts
  g1             Disabled
  g2             Enabled
Single Host Violation: Discard
Trap: Enabled
Frequency: 100
Status: Authorized (Locked)
Counter: 9